TUTTO QUELLO CHE GLI ALTRI NON OSANO DIRTI

n.153

HACKER JOURNAL

www.hackerjournal.it

SOLO 2,00 €

NO PUBBLICITÀ
SOLO INFORMAZIONE E ARTICOLI



eMule
NUOVA VERSIONE

INCHIESTA
SCOPRI LA TARIFFA
Alla ricerca della *MIGLIORE OFFERTA* per il *TELEFONINO DELL'HACKER*

TORNADO
La *NUOVA FRONTIERA* dei programmi pirata

INTERVISTA ESCLUSIVA
GLI ITALIANI SUL TETTO DEL MONDO
Il gruppo di *HACKER* che ha *VINTO IL CAPTURE THE FLAG*

Anno 8 – N.153
12 / 25 Giugno 2008

Editore (sede legale):
WLF Publishing S.r.l.
via Donatello 71
00196 Roma
Fax 063214606

Printing:
Roto 2000

Distributore:
M-DIS Distributore SPA
via Cazzaniga 2 - 20132 Milano

Copertina: Daniele Festa

HACKER JOURNAL
Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

Una copia 2,00 euro

Direttore Responsabile:
Teresa Carsaniga

hack·er (hăk'∂r)
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

editoriale

HACKER JOURNAL

Dichiarazioni private e **pubbliche vergogne**

"Fingere di sapere quando non si sa è una malattia."
Lao-Tzû

Siamo stati zitti fino ad ora e abbiamo lasciato che le acque si quietassero prima di esprimerci sulla questione della pubblicazione delle dichiarazioni dei redditi ma ora è giunto il momento di esprimere la nostra opinione.

Il concetto secondo cui ha agito l'agenzia delle entrate pubblicando sul suo sito le dichiarazioni può anche trovarci d'accordo visto che la trasparenza non può che agevolare il riconoscimento di quei soggetti che cercano di campare alle spalle degli altri non pagando le tasse (visto che questo fanno, usufruiscono di servizi che noi con le tasse paghiamo al posto loro) ma forse si sarebbe dovuto riflettere su un paio di cose:

- l'italianità dei lettori di questi dati: con questo non vogliamo partire con la solita tirata sulle caratteristiche della nostra nazione e dei nostri compaesani ma sicuramente siamo un popolo di pettegoli (le vendite delle riviste di gossip lo dimostrano) e certamente sappiamo trasformarci in un popolo di delatori (e non vorrei addentrarmi negli esempi dolorosi e storici di questo, vedi fine della II guerra mondiale). Alla luce di questo sarebbe stato a tutti chiarissimo che uso sarebbe stato fatto di questi dati nel momento stesso della loro pubblicazione, trova il vicino che ti sta antipatico e magari vota contro l'installazione della parabola condominiale e guarda quanto guadagna così alla prossima riunione gli puoi sbattere in faccia il suo reddito e vediamo se dice ancora di no visto che guadagna più di tutti gli altri del condominio...

- la capacità di assorbimento della rete: chiunque abbia avuto a che fare con la rete per qualcosa di più che cercare una cosa in Google o una strada con viamchelin.com sa che se si immette un dato nel calderone non ne uscirà più e quel dato sarà rintracciabile in rete ancora a distanza di anni. La stessa cosa sta accadendo alle famose dichiarazioni, sulle reti di P2P sono tranquillamente scaricabili e a poco valgono le minacce di condanne e altro, gli utenti che sono interessati trovano il modo, come noi ben sappiamo, di scaricarsele e guardarle con calma.

- Ultimo argomento, ma non certo per importanza la completezza e i filtri per l'analisi dei dati: quello che fa più disperare chi abbia delle conoscenze di informatica è l'ignoranza di base di chi effettua queste operazioni, quello che vogliamo dire è: se proprio vuoi pubblicare questi dati fallo in modo che possano solo essere consultati e non manipolati e riadattati ad uso e consumo di qualsiasi analista, se il tuo scopo è quello della trasparenza basta che metti "NOME-COGNOME-CITTÀ- REDDITO" non indirizzo e altro e soprattutto che lo fai in un formato che permetta solo la consultazione, invece i dati immessi sulla possono essere letti in Excell o con altri fogli di calcolo e questo li rende interessanti e preziosi per chi voglia fare analisi di mercato e non solo...

Insomma, come al solito, quelli che dovrebbero essere i massimi esperti si sono dimostrati dei lameroni e tutti noi che ci spezziamo la schiena davanti al monitor per nottate intere ne subiamo le conseguenze...

The Guilty

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo... Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa! Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

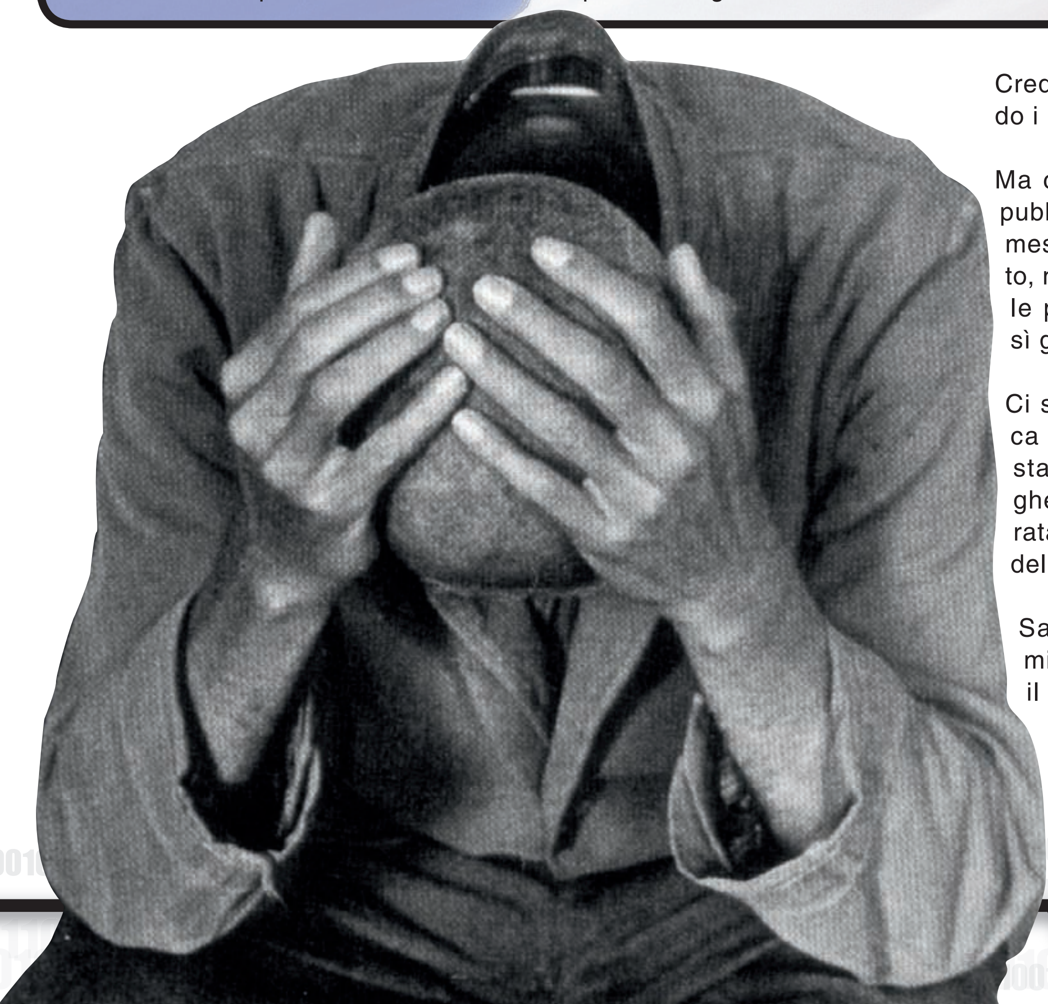
La VIA FRANCESE... sempre più dura

Che il presidente Sarkozy sia un duro non c'è dubbio e che la sua amministrazione abbia dichiarato guerra aperta al P2P è altrettanto certo ma sembra che ora la situazione stia loro sfuggendo di mano...

Il 10 aprile il Parlamento Europeo ha raccomandato ai paesi dell'Unione di non tagliare la connessione internet a chi pratica il filesharing ma il governo francese sembra non aver recepito bene il messaggio tanto che prima delle vacanze potrebbe essere approvato il tanto discusso decreto anti P2P.

La procedura sarà più o meno la seguente:

1° INFRAZIONE: l'utente riceve una lettera di avvertimento dal proprio provider.
2° INFRAZIONE: una commissione di magistrati e funzionari deciderà se staccare o meno la sua connessione, inoltre l'utente verrà inserito in una lista pubblica on-line contenente tutti i rei di P2P. Se il pirata si dichiarerà "pentito, contrito e redento" la sospensione del servizio non supererà i 10 giorni.



Crediamo si stiano davvero superando i limiti della decenza...

Ma come è possibile fare una lista pubblica degli utenti che hanno commesso un reato, certo che è un reato, ma non di sicuro ammazzato delle persone o commesso cose così gravi...

Ci sembra di essere tornati all'epoca delle inquisizioni, dalla Francia sta partendo una caccia alle streghe che ci sembra davvero esagerata nei modi e soprattutto invasiva della privacy delle persone.

Sappiamo di incontri tra il nuovo ministro della Cultura italiano con il suo collega francese e speriamo con tutto il cuore che non sia andato a prendere lezioni di civiltà e dempocrazia da chi non pare proprio aver nulla da insegnare. ■



EXPLORER SENZA CONTROLLO

Un giovane ricercatore israeliano, Aviv Raff, ha trovato un bug in Microsoft Internet Explorer. La vulnerabilità viene sfruttata se è attiva l'opzione Stampa tabella dei collegamenti. Durante la generazione del codice Html necessario per fornire una versione stampabile dalla pagina web, gli Url non vengono validati ma aggiunti così come sono. Approfittando poi del fatto che il processo di stampa appartiene alla zona locale delle impostazioni di sicurezza (meno sicura della zona Internet), uno script malevolo linkato in una pagina può far eseguire al computer codice arbitrario. In Internet Explorer 7 e 8, per fortuna, l'opzione Stampa tabella dei collegamenti è disattivata per default, dunque non si dovrebbero temere attacchi su larga scala.

PIRATE BAY VS MICHAEL JACKSON

Come direbbero i nostri amici romani, "quanto rosicano" queste vecchie star in declino che attaccano The Pirate Bay, famosissimo tracker Bit Torrent ancora in piena attività.
Non bastavano a fargli causa i Village People, gli Ub40, Prince e i detentori dei diritti della musica di Bob Marley, ora ci si mette anche Michael Jackson, il quale ha ingaggiato la Web Sheriff per far chiudere i battenti del P2P. Brokep, noto ammiratore della Pirate Bay, non sembra affatto impressionato dalla lista di questi nomi "autorevoli" nel mondo della musica. "Infatti - dice - il loro è solo un tentativo di prendere dal proprio successo anche l'ultimo centesimo".



Quanto a Michael Jackson, poi, dicono che abbia preso parte al gruppo di accusatori spinto anche dal bisogno di denaro per mantenere il Neverland Ranch, in pericolo a causa dei debiti del suo proprietario e che avrebbe dovuto andare all'asta il 14 maggio.



NAPSTER COTRO TUTTI

Napster, una volta portabandiera del file sharing, P2P, e commercio illegale di Mp3, ha dichiarato che vuole diventare il più famoso negozio online di musica e video musicali nel mondo dichiarando battaglia direttemente ad un colosso del settore come iTunes Stored.
Ha iniziato questa guerra a denti stretti, prima abbattendo i luchetti digitali dei formati Mp3 e poi vendendo i suoi bravi a 0,99 $ e i gli album a partire da 9,95 $. Ben più conveniente del diretto concorrente iTunes. Ma l'arma segreta la sta pensando il presidente, Chris Gorog, cercando di carpire le mancande del mondo Apple per poter rubare milioni di clienti utilizzatori di iPod e company. Aaaahhh... vecchio P2P!

napster®

POMPATI LA RETE!

Trendnet esce in questi giorni con il suo nuovissimo adattatore Powerline Ethernet Adapter.
Questo fantastico apparecchio è capace di raddoppiare la velocità delle reti cablate in modo tradizionale.
Si può attaccare direttamente alla presa della corrente, può essere collegato ad un cablaggio già esistente, supporta la





HOT NEWS

ONNIPRESENTE!

Il futuro delle videoconferenze è sempre più reale e tangibile. A portar bandiera, questa volta, è il nostro "amato" Bill Gates che appare sotto forma di ologramma al World Congress on Information Technology 2008. Un'apparizione virtuale alta più di quattro metri, 4,60 m per essere precisi, che ha impressionato molto i presenti al congresso. Microsoft ha dichiarato che il discorso è stato registrato un paio di settimane fa e che sono molto contenti del successo riscontrato per la prima apparizione dello "zio Bill" in ologramma. Un passo in avanti verso l'onnipresenza a portata di mano.



HP BOCCIA SERVICE PACK 3

Hp consiglia: "Non installate il Service Pack 3". Hewlett-Packard parla così dopo aver visto Microsoft e Amd rimpallarsi la colpa dei continui riavvii dovuti all'installazione del Service Pack 3 di Windows Xp su certi computer. E consiglia così ai suoi clienti di non installare l'aggiornamento.

"Dopo l'installazione della release iniziale del Service Pack 3 per Windows Xp può verificarsi una condizione di errore. L'aggiornamento Service Pack 3 copia sul computer un driver di gestione del risparmio energetico di Intel che non era presente sul computer prima dell'aggiornamento. Durante l'avvio di Windows, i computer con processori Amd possono mostrare un errore con schermo blu". Questo è quando dichiarato da HP. Stiamoci attenti!

SAFARI APRE LE PORTE DEL TUO PC

Safari scarica i file senza il permesso dell'utente. Questo è quello che succede se provate a visitare il sito http://malicious.example.com. Ritrovandovi il desktop pieno di file scaricati di cui non siete a conoscenza.

Il bug sta nella gesione del download. In quanto un sito web malevolo può riempire le directory di default dei file scaricati con tutto ciò che vuole perché Safari "non può essere configurato per ottenere il permesso dell'utente prima che scarichi una risorsa".

Questo crea così un canale di comunicazione tra il web e il proprio PC senza aver la possiblità di controllarlo.

Il problema è stato fatto presente agli sviluppatori di Safari i quali hanno risposto: "Per favore notate che non trattiamo questo come un problema legato alla sicurezza, ma come ulteriore misura per migliorare le difese contro i download involontari".

Ecco le tariffe aeree

Wind, TIM e Vodafone confermano il lancio delle offerte mobili per le chiamate sugli aerei. Wind ha annunciato il suo accordo con Air France, che consentirà di telefonare, inviare SMSin volo. Il Tariffario è di 4 euro al minuto per chiamare, 2 euro al minuto in ricezione e 1,5 euro per SMS. Per TIM, i costi saranno più alti: 3 euro al minuto per le chiamate; 1,90 euro al minuto per ricevere; gli SMS 89 centesimi. Per Vodafone con la Emirates e Qantas, il costo di ogni chiamata sarà di 3 euro al minuto.

crittografia Aes ed ha un'estendibilità massima di 16 adattatori per un colpessivo di 4.800 metri. La velocità è di 200 Mbps (teorici), il doppio di una rete Ethernet tradizionale e supporta i seguenti sistemi operativi: Windows 2000, Xp e Vista) e lo standard Plug and Play.

Tutto quello che serve veramente per potenziare al massimo la tua vecchia rete tradizionale.



Hanno violentato Scribd

Scribd, nato come sito per postare documenti e condividerli con gli altri utenti, è stato innondato dalla pornografia. Migliaia sono, ogni giorno, sono gli upload di materiale vietato ai minori. La direzione fa sapere che presto avverà una coatta epurazione del porno che verà bandito per sempre. La ditta in questione rilascia grosse dichiarazioni: L'erotismo più spinto inficia il valore di Scribd per la comunità scientifica che alimenta il servizio, rischia di distrarre gli studenti che vi attingono e rischia di scatenare la disapprovazione dei genitori degli utenti più giovani. Ma soprattutto, allontana coloro che caricano documenti, la linfa vitale del servizio: non sembrano disposti a veder comparire e diffondere il distillato di anni di lavoro accanto alle immagini di donnine procaci e di dettagliate istruzioni per migliorare le propria virilità". Ed è vero.



DONNE VIRTUALI REALI

Uno studente della New York University, Drew Burrows, stanco di tornare a casa alla sera, tardi, dopo aver lavorato tutto il giorno per poi sdraiarsi da solo in un letto vuoto. Rimasto single da troppo tempo, ha deciso che era ormai necessario trovare una soluzione.
Che cosa dunque potrebbe risolvere meglio questo problema se non una ragazza virtuale? Non si lamenta, aspetta fedele e poi, quando ci si sdraia, cambia posizione e si avvicina, reagendo a ogni mossa del partner umano. L'illusione di trovarsi al fianco una persona vera è così praticamente perfetta, a parte il fatto che manca la terza dimensione. Che peccato!

EMULE DIVENTA NINJA

Solo dopo una settimana dal rilascio dell'ultima versione di eMule 0.49a, la ditta del simpatico mulo si trasforma e diventa ninja nella sua nuove veste di MorphXT 11.0. Ma a dirvela tutta le differenze tra le due versioni sono veramente pochissime. A parte la simpatica anteprima nell'avvio di programma, dove si vede un mulo vestito da ninja che salta sopra i tetti, la nuova versione prevede le modifiche alla gestione dei flussi in entrata ed uscita, dei file posti in condivisione oppure delle modalità con le quali il codice viene compilato per renderlo compatibile con diversi sistemi. Tra le altre modifiche: librerie aggiornate all'ultima versione disponibile, una migliorata compatibilità di MorphXT con Wine,così facendo gli utenti Linux potranno eseguire direttamente il binario per Windows senza ulteriori complicate operazioni di compilazione transpiattaforma. Chi sa dirci invece al livello di velocità di download se ci sono dei sostanziali miglioramenti? Fateci sapere.



VISTA NON CONVINCE GLI SVILUPPATORI

I programmatori software "boicottano" Windows Vista. Un'indagine di Evans Data Corporation, professionisti del mercato statunitense, dichiara che gli sviluppatori sarebbero poco intenzionati a lavorare per Vista. Il 49% di loro sta ancora lavorando su applicativi specifici per Windows XP.
"La questione di fondo è che Vista è stato adottato più lentamente dal mercato, per questo motivo gli utenti corporate e del settore commerciale sono rimasti con XP", ha dichiarato John Andrews, CEO di Evans Data. Per quanto riguarda invece i sistemi operativi alternativi, è confermato l'incremento di interesse nei confronti di MacOS anche se complessivamente continua a trattarsi di un mercato di nicchia.m Nel 2009, comunque, lo scenario dovrebbe cambiare sensibilmente. Il 29% degli sviluppatori rimarrà su XP, ma il 24% passerà a Vista – di fatto l'impegno rispetto al 2008 si triplicherà.

ENERGIA A RISCHIO

Il mese scorso, durante la RSA Conference 2008, gli studiosi avevano il primo appello per far notare la vulnerabilità delle protezioni informatiche degli impianti industriali.
Oggi la Core Security fa sapere, in conferenza stampa, che facilmente si può subire un attacco sulle protezioni messe a favore della gestione dell'energia, delle raffinerie di petrolio che potrebbero venire sabotate dal un semplice attacco lanciato via rete.
I tecnici di Boston hanno capito che è fattibile mandare Suitelink in crash inviando pacchetti dati consistenti ad una determinata porta dei computer che ospitano la piattaforma.

La Wonderware, società che si occupa dello sviluppo del suddetto programma ha detto che rilascerà presto una patch che dovrebbe aggiustare il problema. In realtà la Core Security prevede la scoperta di nuove falle nelle prossime settimane.

CHIMERA SI, CHIMERA NO.

Il Regno Unito dal il suo via libera per la creazione di esseri composti da DNA umano e cellule animali.
Il Parlamento si è espresso favorevole la ricerca sulle cellule staminali basata sulla creazione degli embrioni chimera.
Questi embrioni sono formati da microparticelle di DNA umano che viene innestato nelle cellule animali svuotae del loro gene iniziale. Gordon Brow, che era noto per il suo favoritismo all'esperimento, dice che questo



HOT NEWS

METAL GEAR SOLID NON TRAMONTERÀ

Metal Gear Solid 4 non è il capitolo finale della fortunata serie Konami, così dice Ryan Payton degli studi Kojima Production, durante un'intervista.



"Guns of the Patriots", però è la fine di Solid Snake, un'avventura durata una decina d'anni con la prima console Sony. Un probabile Metal Gear Solid 5 presenterà un nuovo protagonista e una trama tutta nuova, mantenendo però inalterati, sempre secondo Ryan, gli elementi chiave che hanno decretato negli anni il successo della serie.
Gli appassionati più sfegatati saranno contenti di questa notizia, anche se abbandonare totalmente un vecchio e affezionato eroe è sempre rischioso.
La sfida per gli ideatori è grande, ma un nuovo successo è dietro l'angolo...

LA CONSOLE TI UCCIDE

Greenpeace accusa le console. Nell'ultima operazione di Greenpeace, "Playing Dirty", ha riscontrato che tutte e tre le console sono risultate positive all'uso di materiali chimici pericolosi, sebbene in linea con le normative in materia dell'Unione Europea. Le console, secondo Greenpeace, contengono diversi materiali chimici come la resina polivinilica (PVC), i plastificanti, il berillio e il bromo.
Insomma dei veri e propri "depuratori" di tossine. Hanno, inoltre trovato alte quantità di bromo in tutte e tre le console, mentre Xbox 360 e PS3 contengono livelli molto elevati di plastificanti, che non sono permessi all'interno dell'Unione Europea in prodotti per bambini e nei prodotti da gioco. I test hanno mostrato che i tre produttori hanno comunque ridotto o eliminato l'uso di alcune sostanze altamente tossiche contenute in passato.



IL BOLLINO DI AMD

Il PC da gioco? Quello AMD ha il bollino AMD Game! è stata pensata per aiutare i consumatori a scegliere il PC adatto per giocare ai titoli videoludici più recenti. Per contraddistinguere tali sistemi, i produttori utilizzeranno il logo AMD Game! più un secondo bollino che specificherà la classe di potenza di quel PC (standard o ultra), il tipo di processore e la tecnologia grafica utilizzata. I requisiti hardware minimi sono costituiti da una CPU Athlon X2 5600+, un processore grafico ATI Radeon HD 3650 e un chipset AMD 770 o Nvidia nForce 500. Per essere identificato come Ultra, un PC deve invece montare almeno un processore Phenom X4 9650, una GPU ATI Radeon HD 3870 e un chipset AMD 770.



studio probabilmente darà la possibilità di sviluppare lo studio di cure per malattie genetiche degenerative.
Non sono mancate, naturalmente, le polemiche della bigotta Chiesa Cristiana che dichiara per voce del cardinale Keith O'Brien: Tutto ciò è un attacco mostruoso ai diritti umani, alla dignità delle persone e alla vita". Difficile è stabilire chi ha torto e chi a ragione in fatto di etica, ancor di più se quando devi decidere l'approvamento di questo decreto ti ricordi che tua figlia è una di quelle persone con tali malattie. Come la figlia del premier inglese.

OFFICE K.O.

L'Office di Microsoft fa acuq da tutte le parti. Si pensi solo che in questo mese sono state rilasciate 4 pacht per risolvere problemi su prodotti Microsft, tre delle quali erano tutte per il pacchetto Office.
Le vulnerabilità riguardanti Office colpiscono tutte le versioni per Windows dalla 2000 alla 2007, oltre alla 2004 e alla 2008 per Mac.



Una riguarda la gestione del formato .rtf (Rich Text Format); la seconda i fogli di stile; la terza, infine, colpisce Publisher e permette a un attaccante di prendere il controllo un un Pc tramite un documento appositamente creato che venga aperto dall'utente vittima.
Insomma, meglio mettersi ai ripari prima di essere completamente tirati giù.

eMule si rinnova

A sette anni dalla sua nascita, il più famoso programmadi file sharing non perde un colpo e si presenta in una nuova versione ancora più potente



Sin dalla sua nascita, eMule è in una versione "provvisoria". La versione ufficiale, infatti, è ancora indicata come 0.48a ma, nonostante questo, è usata da milioni di persone. Ora gli sviluppatori del celebre programma hanno rilasciato la versione 0.49a, che introduce alcune interessanti novità e segna un grande passo avanti nell'evoluzione dei sistemi peer to peer.

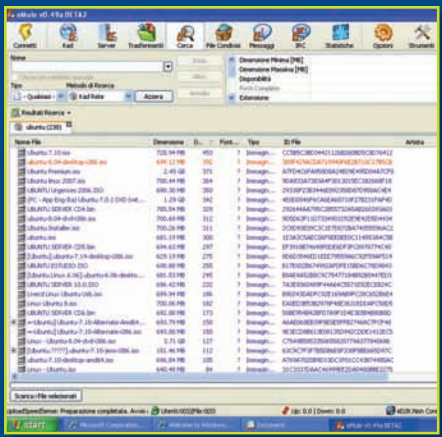
:: Tempi stretti

Come la maggior parte delle applicazioni Open Source, eMule non garantisce un calendario per l'avanzamento dei lavori, ma ormai con una scadenza piuttosto precisa gli sviluppatori propongono un aggiornamento ufficiale o una nuova versione Beta. In questa occasione hanno deciso di adottare il sistema della beta pubblica, alla quale è seguita dopo pochi giorni dalla verisone ufficiale. La pubblicazione della verisone definitiva è stata annunciata proprio quando Computer Magazine sta per chiudere il numero e i test citati in questo articolo sono stati effettuati con la verisone Beta del programma. Dai controlli fatti, però, le due versioni risultano pressochè identiche.

Nel corso delle nostre prove, la versione beta 2 non ha dato alcun segno di cedimento nemmeno dopo un periodo di utilizzo costante. Del resto la nuova versione di eMule poggia su basi solide: l'architettura del software è ormai estremamente rodata e le centinaia di forum Internet animati dagli appassionati di peer to peer hanno permesso di individuare e risolvere tutti i problemi che si sono presentati nel corso degli anni, arrivando a risolverne la maggior parte. La tempestività con cui è stata rilasciata la versione ufficiale, d'altra parte, lo conferma.

:: Piattaforma di prova

Visto che buona parte delle novità introdotte dalla nuova versione di eMule sono nella gestione delle connessioni e sono volte ad aumentare la sicurezza dei trasferimenti, Computer Magazine ha deciso di effettuare le prove mettendo a confronto la versione ufficiale 0.48a e la nuova 0.49a. Per farlo sono state create due macchine virtuali identiche e ospitate sullo stesso



Il motore di ricerca non è cambiato rispetto alle versioni precedenti. L'unica variazione è che ora le finestre di ricerca aperte vengono conservate anche se chiudiamo e riapriamo il programma.

computer dotato di processore Dual Core. L'ambiente virtuale simula alla perfezione la condizione più difficile per un programma P2P, ovvero quella di dover superare diversi livelli di firewall e router per stabilire le connessioni. In questo modo è stato possibile verificare una delle novità annunciate, ovvero la migliorata gestione dei collegamenti attraverso reti protette. Le due macchine virtuali, che contenevano solo Windows XP SP2 e la versione di eMule assegnata, sono state avviate contemporaneamente e il programma all'interno è stato lanciato con il minimo scarto possibile in modo da avere un riscontro visivo immediato delle variazioni.

:: Novità annunciate

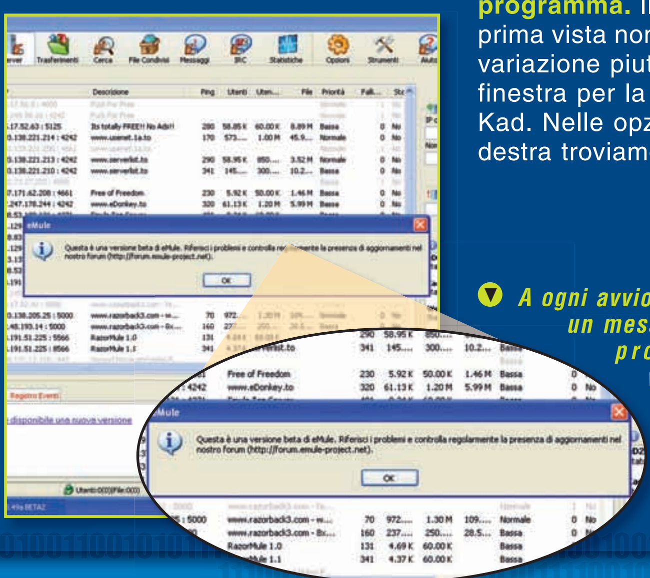
La maggior parte delle innovazioni introdotte nella versione 0.49a beta 2 riguarda la rete Kad, quella che permette di scambiare file e informazioni senza bisogno di utilizzare i server. Questa funzione, introdotta a partire dalla versione 0.40, ha riscosso un successo sempre più grande grazie alla maggiore riservatezza che offre rispetto al "vecchio" meccanismo basato sui collegamenti ai server. Quest'ultimo, infatti, soffre di tutti i difetti che affliggono i sistemi centralizzati, fra cui anche una certa rintracciabilità delle connessioni poco gradita a chi scambia abitualmente file tramite Internet.

Le maggiori novità in questo campo riguardano una migliore gestione delle connessioni anche in presenza di firewall o router, protezione dal sovraccarico e una revisione del codice che ne migliora le prestazioni. Anche il sistema dei messaggi è stato rivisto in modo da ridurre il fastidioso fenomeno dello spam. Inoltre, è stata aggiunta una funzione per conservare le ricerche attive dopo lo spegnimento del programma e sono state fatte alcune modifiche al sistema di controllo per rendere più agevoli e immediate alcune operazioni frequenti.

:: Sul campo

Al primo avvio della nuova versione ci accoglie l'abituale procedura guidata per la configurazione del programma. Il sistema di controllo a prima vista non cambia molto: l'unica variazione piuttosto evidente è nella finestra per la connessione alla rete Kad. Nelle opzioni di connessione a destra troviamo una nuova voce che si chiama nodes.dat dall'URL. Si tratta di una funzione che permette di impostare un indirizzo Internet per il lancio delle connessioni tramite la rete Kad, in modo simile a quanto succede con il file Server.met per i server.

In pratica, questo strumento permette un avvio più pratico delle connessioni in questa particolare rete. Normalmente, infatti, la connessione alla rete Kad sfrutta un elenco dei client che il programma ha contattato di recente. Quando nessuno di questi risulta online, però, il circuito Kad non si avvia ed è necessario collegarsi a un server eDonkey. Grazie all'introduzione di questa funzione, invece, il programma è ora in grado di accedere sempre alla rete Kademlia senza che ci sia più bisogno di "appoggiarsi" al più vecchio e fragile sistema dei server.



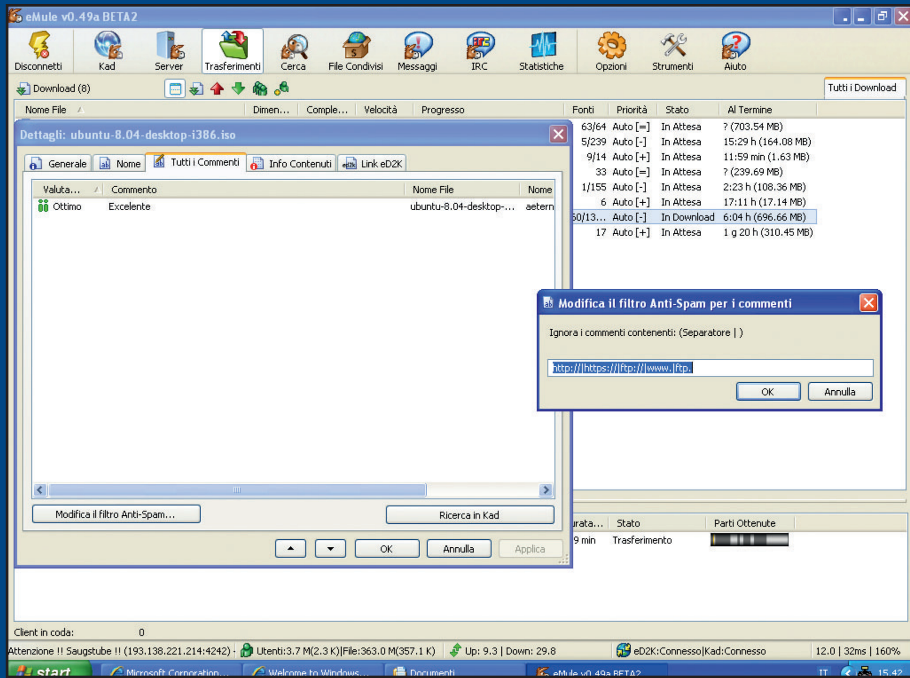
A ogni avvio di eMule 0.49a Beta 2, un messaggio ci avvisa che il programma non è una versione definitiva. L'invito a segnalare eventuali problemi permetterà agli sviluppatori di individuare più in fretta eventuali difetti.

ADDIO AI SERVER...

Se usiamo abitualmente eMule ci saremo sicuramente accorti che molti dei server "storici" non risultano raggiungibili da molto tempo e che in generale il numero di quelli disponibili si è decisamente ridotto negli ultimi tempi. Questo deriva da una serie di cause, in parte tecniche e in parte legali. Dal punto di vista tecnico con il progresso delle connessioni veloci diventa sempre meno necessario avere a disposizione un server perennemente connesso. Statisticamente, infatti, è molto probabile che diversi client si "incrocino" online vista la maggiore permanenza in Internet. Dal punto di vista legale invece, dopo il sequestro dei server Razorback avvenuto all'inizio del 2006 in Belgio, la situazione dei gestori dei server è diventata piuttosto complessa e sempre meno persone accettano di accollarsi le responsabilità della gestione.

Il successo di Kad

Il protocollo Kad, introdotto in eMule dalla versione 0.40, è estremamente efficace e soprattutto permette l'uso del programma indipendentemente dalla presenza di server centrali. Anche se dal punto di vista di chi usa il programma questo sistema non presenta particolari difficoltà, in realtà il principio tecnico sul quale si basa è piuttosto complesso. In termini tecnici la rete Kad è un'implementazione del protocollo Kademlia, che a sua volta è lo sviluppo di una Tabella di hash distribuita specifico per reti Peer to Peer. Il vantaggio di questo sistema è che permette un raggiungimento capillare di ogni client della rete garantendo nello stesso tempo un buon livello di anonimato. In pratica i client si scambiano le informazioni sfruttando una specie di "tabella di prossimità" che stabilisce dove sono reperibili i frammenti di file che servono senza conoscere la posizione della parte intera e senza scambiare gli indirizzi IP dei PC. Un notevole sviluppo che ci permette di scambiare file in modo molto più sicuro rispetto ai server tradizionali.



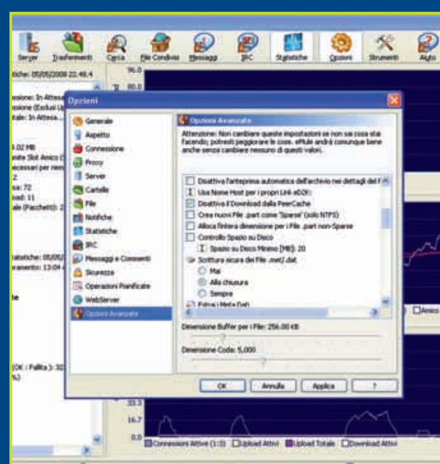
È possibile modificare direttamente il filtro antispam senza dover ricorrere alla finestra delle Opzioni. Possiamo accedere all'impostazione attraverso un pulsante che si trova nella finestra dei commenti.

:: Rete veloce

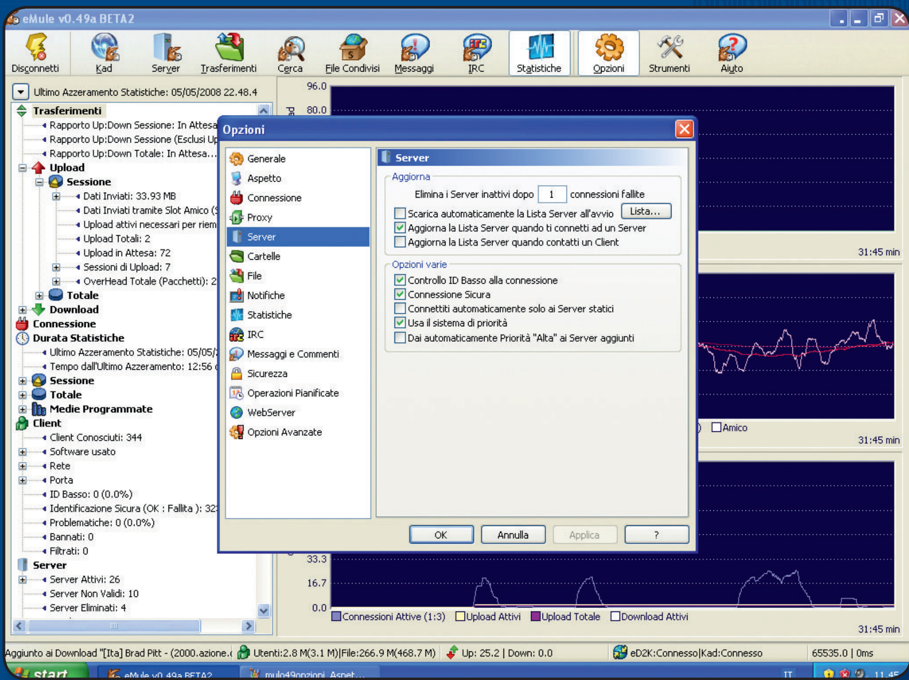
A parità di condizioni con la versione precedente, l'edizione 0.49a richiede un tempo più lungo per la connessione ai server, dovuto probabilmente a una revisione del codice realizzata per garantire una maggiore sicurezza dei collegamenti. In compenso il lancio delle connessioni Kad risulta più rapido ed efficiente. Dal punto di vista delle ricerche non è cambiato molto, se non la possibilità di mantenere archiviate quelle attive anche spegnendo e riavviando il programma. In compenso, una volta messo in coda il file notiamo una certa differenza nella gestione delle risorse. La versione 0.49a infatti mostra un minor numero di fonti raggiungibili, ma nello stesso tempo voti e commenti compaiono sul nostro schermo in modo molto più rapido. Un'ottima notizia, visto che i commenti rappresentano lo strumento più efficace per individuare ed evitare di scaricare le numerose "bufale" che circolano sul Web. Anche la velocità di download è mediamente più veloce, anche quando disponiamo di un ID basso. Probabilmente il codice è stato rivisto in modo da essere un po' più "selettivo" nei confronti delle fonti di dubbia provenienza e consente così di ottimizzare l'utilizzo della banda.

:: Piccoli accorgimenti

La nuova versione di eMule presenta senza dubbio qualche modifica importante, ma non segna un cambio epocale. Al di là di alcune variazioni nel protocollo e nella migliore gestione della rete Kad, le variazioni riguardano soprattutto la risoluzione di alcuni piccoli difetti e una maggiore attenzione alla sicurezza. Per esempio, ora le impostazioni predefinite prevedono la connessione sicura ai server, che prima era prevista solo come opzionale. Fra le modifiche annunciate per la versione definitiva, ma ancora in fase di sviluppo, c'è anche una parziale protezione delle cartelle



Come impostazione di base ora il download dalla PeerCache è disabilitato. Sono ben pochi, ormai, i server proxy che conservano frammenti di file per consentire un download più rapido.



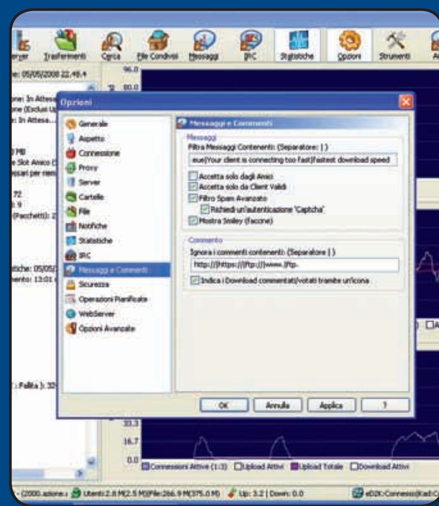
Fino alla versione 0.48, le impostazioni predefinite non prevedevano la connessione sicura per i server. Oggi invece è normalmente attiva, segno della maggiore diffidenza nei confronti di questo tipo di servizio.

personali e un migliore supporto per la funzione Universal Plug & Play. Quest'ultima dovrebbe migliorare le procedure automatiche per "aprire" le porte dei router e ottenere così migliori prestazioni in fase di ricerca e di trasferimento dei file. Si tratta però di un aggiornamento i cui effetti benefici sono piuttosto difficili da verificare nella pratica.



:: Addio alla cache

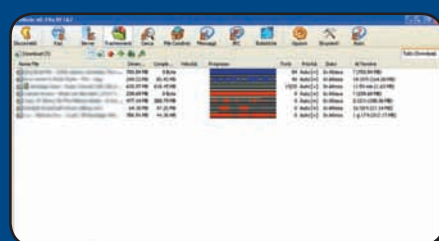
Le impostazioni predefinite, inoltre, non prevedono più l'uso della funzione PeerCache. Si tratta, in pratica, di un sistema che sfrutta dei server proxy ai quali è affidato il compito di agire come intermediari e memorizzare i dati in trasferimento. Grazie a questo sistema, i server proxy agiscono come "serbatoi" e forniscono direttamente i dati ai computer che li richiedono, migliorando le prestazioni del programma e riducendo il traffico "inutile" sul Web. Anche se in teoria la funzione può offrire vantaggi notevoli, richiede l'uso di macchine dedicate esattamente come i server usati per la connessione nella tradizionale rete eDonkey. Una filosofia, questa, che ha mostrato tutti i suoi limiti negli ultimi anni e che gli sviluppatori di eMule hanno ormai abbandonato.



Il nuovo sistema di autenticazione Captcha impedisce ai sistemi di spam automatico di intasarci di messaggi. In questo modo probabilmente il sistema di messaggistica tornerà in voga.

:: Senza traumi

Come accade per tutte le versioni di eMule l'installazione della versione 0.49a non altera in alcun modo i download parziali e le impostazioni. È sufficiente trasferirli come al solito copiandoli nelle cartelle di eMule, per ricominciare a scaricare i nostri file come se niente fosse. Se invece vogliamo provare la nuova versione senza disinstallare quella vecchia, ricordiamoci di cambiare la cartella di destinazione, altrimenti sovrascriverà automaticamente quelle precedenti.



All'apparenza il numero di fonti ci sembra svantaggioso, ma basta attendere che i download si avviino per renderci conto che il download è più rapido.

Attacco via Firewire



I rischi delle connessioni veloci e dell'accesso diretto alla memoria. Non solo su Windows

A cura di MacHack.it

All'inizio di marzo una testata australiana ha dato spazio ad un'insicurezza di Windows ed al ricercatore che l'ha scoperta. La tecnica divulgata si basa sulla lettura e scrittura di dati riservati tramite un collegamento Firewire ed a divulgarla è stato il neozelandese Adam Boileau. Vediamo meglio in cosa consiste e quali sono i rischi.

:: Accesso alla memoria

La tecnica è stata diffusa da Adam Boileau e prevede il collegamento di un portatile con Linux ad una macchina Windows in esecuzione, accedendo direttamente alla memoria di quest'ultimo per leggere e intervenendo su password o altri codici di accesso.



Anche se l'insicurezza è stata giocoforza accomunata a quella diffusa nello stesso periodo che permette di leggere i dati sulla memoria "volatile" anche dopo un riavvio, l'attacco via Firewire ha un'origine molto più vecchia. Boileau già due anni fa, alla manifestazione Ruxcon 2006 (http://www.ruxcon.org.au/presentations.shtml#14) aveva tenuto una presentazione dal titolo "Hit By A Bus: Physical Access Attacks With Firewire" (http://storm.net.nz/static/files/ab_firewire_rux2k6-final.pdf) ed aveva avvertito Microsoft della vulnerabilità. Dopo che a Redmond hanno nicchiato per due anni, il ricercatore ha deciso di rendere disponibili gli strumenti creati per evidenziare la questione irrisolta.

:: Gli strumenti

Sul blog di Boileau (http://storm.net.nz/projects/16) si trovano i software usati come anche diverse spiegazioni. Tra queste il fatto che i tool sono efficaci su qualsiasi computer bersaglio con porta IEEE1394 (il nome canonico di Firewire, talvolta chiamato anche iLink) e che l'accesso non è un bug ma una caratteristica propria del tipo di connettività in oggetto.



Nella pratica chi volesse provare deve collegare fisicamente un computer con sistema operativo GNU/Linux alla

macchina target. A questo punto si può usare qualcuno degli strumenti scaricabili dal sito. Ad esempio winlockpwn è un'utility in PyThon che aggira la password di macchine Windows con lo schermo bloccato.
bioskbsnarf invece è un tool usato nella presentazione del 2006 da Boileau per scoprire la sua stessa password di BIOS. Il codice, sempre in PyThon, analizza un device tipo /dev/mem oppure un'immagine della memoria già acquisita via FireWire.
Quest'ultima operazione si può fare con "1394memimage", uno degli strumenti inclusi in pythonraw1394-1.0.tar.gz pacchetto compresso da 447kB che include anche romtool e altro ancora.
Il tutto è dato per funzionante su una Debian Sarge con controller OHCI 1394 e supporto per Firewire a livello di kernel.

:: Un vecchio baco... nella mela

Il "problema" di poter leggere e scrivere la memoria di un altro computer via Firewire/IEE 1394 non è un bug ma una caratteristica voluta e nota e questa "vulnerabilità" esiste in tutti i sistemi operativi. L'implementazione corretta delle specifiche contempla il DMA (Direct Memory Access) e quindi vantaggi e svantaggi su varie piattaforme: Windows, Linux e... Mac OS X.
L'idea di sfruttare la connessione Firewire per accedere alla memoria di un altro computer ha origine proprio sui computer di Apple, che ha ideato questo tipo di connessione, poi trasformata in uno standard.



Nel 2002 alla manifestazione Mac Hack uno smanettone noto come "Quinn The Eskimo" si aggiudicò il premio come migliore hack mostrando alla platea un particolare salvaschermo che poteva "imporsi" su qualsiasi Macintosh collegato via Firewire.

FireStarter (http://www.quinn.echidna.id.au/Quinn/WWW/Hacks.html#FireStarter) può generare una schermata con delle fiamme su una serie di Macintosh dell'epoca (ma il supporto si può espandere): nella pratica il software accede alla VRAM (la memoria video) riesce ad indovinare l'indirizzo giusto del buffer e ci scrive i dati, usandolo come terminale (grafico) remoto.

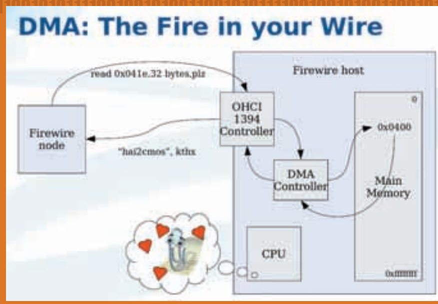
:: Basta anche un iPod

Il lavoro di Boileau su Windows si basa su quello di un tedesco, Max Dornseif, che nel 2004 e poi ancora nel 2005 in vari convegni (http://md.hudora.de/presentations/#firewire-pacsec) ha mostrato una variante furba quanto alla moda della vulnerabilità: usare un iPod.

All'epoca i player digitali di Apple usavano prevalentemente la FireWire e caricando sul dispositivo un OS Linux il piccolo mattoncino bianco poteva addirittura trasformarsi in un logger di tutto ciò che succedeva sullo schermo computer bersaglio salvandolo come video a 10fps. Il risultato delle dimostrazioni di Dornseif era che la domanda "ehi, posso collegare il mio iPod al tuo PC per ricaricarlo?" assumeva una luce nuova.

:: La soluzione

Come scritto Firewire/IEE 1934 ha bisogno del DMA perché a differenza di USB consente a più device di comunicare direttamente senza l'assistenza di una CPU che faccia da "arbitro": si tratta di una caratteristica insita nello standard e l'unica soluzione generale e universale sarebbe quella di rivedere le specifiche.



Una schermata del meccanismo con cui si accede direttamente alla memoria.

Questo non vuol dire che il problema non sia risolvibile. Apple senza troppo rumore ha modificato il suo sistema operativo di modo che se si abilita la password sull'Open Firmware (di cui abbiamo parlato sul numero 135 di Hacker Journal) la Firewire non è più suscettibile ad attacchi.
A partire da Darwin v6.2/Mac OS X 10.2.2 (http://rentzsch.com/macosx/securingFirewire) è stato modificato il codice in IOFireWireFamily. Questo controlla se la password sull'Open Firmware è abilitata e in caso affermativo non è più possibile l'accesso diretto alla memoria via Firewire e FireStarter non funziona più. Per la cronaca la patch di Apple risale al novembre 2002, casualmente un paio di mesi dopo la presentazione del salvaschermo invasivo di Quinn.
E sugli altri computer? Beh, in attesa di una soluzione software c'è chi consiglia di tappare in qualche modo le porte Firewire. ■

IL RISCHIO EFFETTIVO

Oggettivamente la Firewire non è così diffusa al di fuori del mondo Apple e di alcuni computer di marca o quelli votati all'audio o video professionali, dove l'USB sinora si è mostrato spesso inadeguato. Se la porta non c'è il rischio è nullo. A meno che il bersaglio non sia un portatile. C'è il rischio che l'attaccante infili una schedina di espansione Cardbus o Expresscard e visto che anche hanno il DMA...

I pirati cinesi campioni di ingenuità?

Alcuni hacker cinesi avrebbero attaccato Internet per manifestare il loro malcontento sulle discussioni relative ai diritti umani in Cina



I pirati cinesi sono degli ingenui? I combattenti digitali della Grande Muraglia si muovono sulla Rete come semplici "script kiddies", a colpi di attacchi "Denial of Service" (DDoS) e altri virus senza usare i proxy? Alcuni hacker cinesi avrebbero attaccato siti e server Internet appartenenti a gruppi occidentali di Paesi che hanno parlato della situazione dei diritti umani in Cina. A fine aprile, per esempio, un programma virus è stato diffuso a partire dal sito di Reporters Sans Frontières. Si tratta di un programma-spia scaricato da un sito di Taiwan. "Era stato installato anche un sistema di amministrazione pirata" - ha confermato il servizio stampa di RSF. La catena di distribuzione Carrefour minacciata da un attacco DDoS, la rete di informazione CNN attaccata... Sono decine i siti infiltrati. E in tutti i casi gli IP provenivano dalla Cina.

"Attacchi di grandi proporzioni provenienti dalla Cina ma coadiuvati anche da 'bot' hanno colpito i siti di Carrefour in tutto il mondo" - conferma una fonte della redazione. Un attacco non molto discreto: i bot utilizzavano IP controllati da provider cinesi. Un fatto strano e troppo semplice.



Da parte sua, la catena americana CNN è stata colpita più volte da attacchi DDoS. A fine aprile ha subito tre giorni di bersagliamento. Questi tentativi di blocco erano di piccola entità e non hanno preoccupato particolarmente il sito americano, che tuttavia ha dovuto chiudere per qualche ora il suo portale sportivo. All'attacco ha preso parte un gruppo di "hacker-attivisti". Questi ultimi, battezzatisi HackCNN, hanno messo on-line un sito che offre programmi "pirata" per il lancio di attacchi DDoS. La pagina "Sport Network" (sports.si.cnn.com - sportsnetwork.com/) è stata gratificata di un vistoso messaggio "Tibet was, is, and always will be a part of China!" (Il Tibet era, è e sarà sempre parte della Cina!). CNN ha dovuto chiudere questo spazio per 24 ore, esponendo un laconico messaggio di scusa: "Sports Network, come altri grandi siti di attualità, è stato attaccato da un soggetto politico cinese e di conseguenza è temporaneamente inaccessibile. Siamo spiacenti dei disagi causati e torneremo on-line appena sarà possibile".

:: I pirati: tutti cinesi?

I servizi segreti dello Zio Sam parlano di pirati di età compresa tra i 20 e il 25 anni; si tratterebbe di studenti. HackCNN distribuiva diversi programmi allo scopo di disturbare la CNN, tramite il sito www.hacknn.com. Il sito è stato chiuso. Il primo programma, denominato AntiCNN.exe, consentiva di sommergere il server della CNN di richieste di http. Il secondo, Sdos.exe, dava la possibilità di specificare un server e una porta per l'attacco. Una pioggia di dati inondava quindi il TCP del sito attaccato. Il terzo programma era truccato. "Si trattava di una backdoor che avrebbe consentito ai pirati che la diffondevano di infettare i pirati che la utilizzavano" - conferma José Nazario di Arbor Networks.





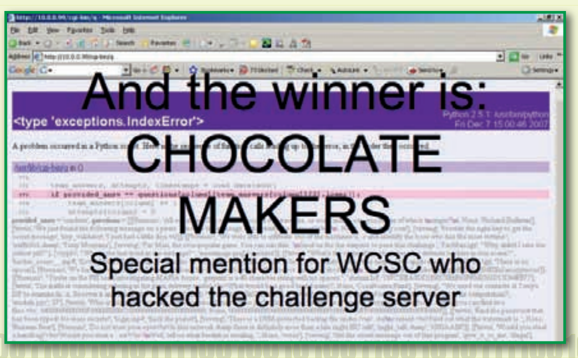
Insomma, questi pirati sono cinesi o no? Altrettanto stupefacente è il fatto che questi "pirati" e "hacker" cinesi non conoscessero nemmeno l'abc della pirateria, che consiste nell'utilizzo di proxy. È un po' come se avessimo la possibilità di entrare nella Banca d'Italia senza essere visti e di servirci direttamente dalle casse e invece preferissimo indossare un abito da discoteca a pallini e appenderci al collo un cartello con scritta la nostra identità. E tutto questo, naturalmente, assaltando la banca in pieno giorno. Nemmeno il più sciocco degli "script-kiddies" agirebbe in questo modo; figuriamoci dei pirati al soldo del governo di Pechino!

Essere Hacker Oggi

Molto tempo è passato dai primi voli del Condor è gli hacker sono cambiati, scopriamo come con un'intervista alla crew italiana che ha vinto il Capture the Flag



Una volta definirsi Hacker aveva un gusto particolare. Gli Hacker erano figli di una corrente di pensiero nuova, primigeni della tecnologia e antagonisti naturali di quelle regole che volevano il mondo digitale imbrigliato e guidato da un'autorità centrale massificante, fredda, calcolatrice. Generalmente non erano affatto "cattivi" come sono stati dipinti dalla stampa e solo raramente sono stati dei fuorilegge. Negli anni in cui ebbero la massima visibilità, il Condor imperversava indisturbato per i server governativi americani e non era ancora stato catturato dalla FBI. Avevano costruito il proprio immaginario su film come Wargames e sui romanzi di Gibson,

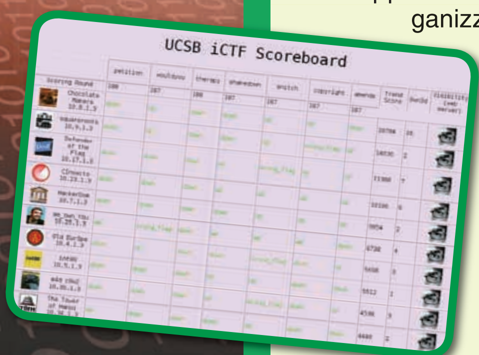


stavano già abbandonando le BBS e le Packet Radio, in cui era nati, per migrare in massa verso una Rete sempre più diffusa e capillare. Un mondo promettente apriva le proprie porte, un mondo in cui le utopie apparivano ancora realizzabili. Gli Hacker erano alfieri di un universo immenso di conoscenze, condiviso e senza alcun tipo di restrizioni. Adesso che i teenager di allora sono trentenni e quarantenni, alcuni dei quali hanno fondato floride aziende ITC, appare naturale chiedersi chi siano i nuovi Hacker. Per saperlo abbiamo deciso di intervistare un gruppo di loro, per l'esattezza i Chocolate Makers, vincitori di un'importante contest internazionale.



1) Ormai vi conoscono in molti, avete vinto l'edizione 2007 del "Capture the Flag", una competizione mondiale fra gruppi di Hacker. Come si svolge la gara? Come avete ottenuto il prestigioso titolo? Qual è stato il gruppo più duro da battere e perché?

Gli organizzatori della gara preparano l'immagine virtuale di un sistema nel quale sono state inserite applicazioni, scritte ad-hoc per la competizione, che contengono una o più vulnerabilità. L'immagine della macchina virtuale è quindi distribuita a tutti i partecipanti. Il compito delle varie squadre è quello di studiare le applicazioni sviluppate dagli organizzatori, trovare le vulnerabilità, correggerle sulle proprie macchine e, infine, utilizzarle per compromettere le macchine degli avversari. È da diversi anni che partecipiamo a questo genere di competizioni e siamo quasi sempre riusciti ad ottenere buoni piazzamenti.. quest'anno ci è andata meglio del solito! In questo tipo di gare, i gruppi più forti sono solitamente quelli europei, in particolare austriaci e tedeschi.



2) Potete svelare l'aneddoto che si cela dietro al nome "Chocolate Makers" con cui avete battezzato il vostro gruppo?

La prima volta che abbiamo partecipato ad una gara di



LA STORIA

Il gruppo dei "Chocolate Makers" è formato da studenti, dottorandi e docenti dell'Università degli Studi di Milano. Il LaSER, il Laboratorio di Sicurezza e Reti di cui fanno parte i membri del gruppo, è nato intorno al 2000 da un'iniziativa del Prof. Danilo Bruschi, che ne è tutt'ora il responsabile. Da allora, il laboratorio è sempre stato all'avanguardia nella ricerca nell'ambito della sicurezza informatica. I "Chocolate Makers" hanno iniziato a partecipare alle competizioni di hacking nel 2004, in occasione di una delle prime edizioni dell' "International Capture the Flag". Negli anni successivi si sono susseguiti diversi membri: alcuni hanno intrapreso la carriera lavorativa, mentre altri hanno proseguito i propri studi all'estero, dove la sensibilità e l'interesse per la sicurezza informatica sono spesso maggiori. Oggi, il Laboratorio LaSER rappresenta uno dei principali centri di ricerca italiani nell'ambito della sicurezza informatica.



questo tipo pensavamo di classificarci tra gli ultimi, facendo la "figura dei cioccolatai".. e da qui abbiamo preso il nome!

3) Ormai chi dice Hacker dice tutto e non dice niente. Il termine ha troppi significati per poter essere chiaro ed auto-esaustivo. Secondo voi, cosa è un Hacker?

Un "hacker" è semplicemente una persona curiosa di sapere perché e come funzionano le cose, fin nei minimi dettagli. La massima aspirazione di un "hacker" è dimostrare di essere in grado di fare cose che altri ritengono estremamente difficili. Il termine non è ovviamente circoscritto alla sola sicurezza informatica, come dimostrano le varie competizioni ospitate in manifestazioni stile DefCon.

4) Come convivono le due nature che vi animano, quella dell'Hacker e quella del Ricercatore? Quanto vi sprona la sfida e quanto il desiderio di conoscere?

"Fare ricerca" crediamo voglia dire cercare di contribuire al progresso di un particolare settore scientifico. Un simile obiettivo è certamente molto vicino al concetto di "hacking".

5) Una volta, chi diventava Hacker lo faceva seguendo un percorso ideologico particolare, diciamo di "controcultura". Quali sono le differenze rispetto al passato? Quanto un Hacker differisce dall'Esperto di Sicurezza che opera, magari, in una multinazionale?

Le motivazioni che spingono una persona a cercare di diventare un hacker sono probabilmente le stesse di vent'anni fa, siano esse ideologiche o puramente "tecniche". La differenza principale è che, adesso, ci sono molte più persone, erroneamente definite "hacker" dalla stampa, che sfruttano problemi di sicurezza unicamente per scopi di lucro. Un esperto di sicurezza di una multinazionale può o meno essere un hacker, indipendentemente dal lavoro che fa.

6) Quali sono, secondo voi, i principali nodi che dovrà dipanare l'evoluzione digitale nel solco dell'etica informatica? Quale ritenete debba essere il percorso da intraprendere, ad esempio, in merito alla tutela del diritto d'autore e della privacy nonché per combattere la censura delle informazioni operata sulla Rete?

Non crediamo esista un' "etica informatica" così distinta dall'etica del "mondo reale". I problemi che è necessario affrontare sono sostanzialmente gli stessi, solo che vengono notevolmente amplificati dalle potenzialità degli strumenti informatici.

7) I giornali spesso creano allarmismo. Mettiamo un punto sulla questione: quali sono i rischi concreti che corre un "utente domestico informatico medio"? Qualche consiglio per vivere al riparo dalle maggiori insidie?

I giornali non creano abbastanza allarmismo! Basta vedere quanto poco si tiene conto della sicurezza informatica nelle aziende. Anche un utente domestico corre molti rischi: furto di identità, dati personali oppure quello di venire infettato da un malware e entrare a far parte di una botnet, che verrà affittata su eBay al miglior offerente per le più svariate azioni illegali. Il problema di fondo è che un computer è uno strumento estremamente complesso, che non può essere utilizzato senza consapevolezza dei pericoli che si possono correre.. è un po' come voler guidare una macchina senza patente!

8) Quali sono le principali tecniche d'attacco che si stanno affermando in questo periodo? Volete dare qualche consiglio agli amministratori di sistema?

Negli ultimi anni abbiamo assistito ad una diffusione capillare delle applicazioni web: oramai quasi tutt i siti hanno contenuti dinamici, e spesso il compito di realizzare le applicazioni per l'erogazine di quest'utlimi è affidato a programmatori con scarse competenze di sicurezza. È quindi ovvio che la maggior parte delle vulnerabilità in circolazione riguarda proprio le web application. Più che gli amministratori di rete, sarebbe opportuno sensibilizzare aziende e sviluppatori sull'importanza della formazione sulle tematiche di sicurezza. Il problema è che investire nella sicurezza spesso non porta a guadagni immediati e tangibili.. ■

Prepariamoci al peggio con un'E-MAIL

Un servizio di consegna messaggi in automatico e con la sicura. Per cautelarsi in caso succeda qualcosa o come sistema di avvertimenti

La formula è semplice quanto utile: JustInCaseIDie.com (http://www.justincaseidie.com/) permette di creare un messaggio che verrà inviato ad un singolo indirizzo email dopo un tempo a scelta, a meno che non lo si disdica. L'idea di base, rafforzata dal dominio scelto, è quella di lasciare un messaggio pronto che verrà inviato ad un caro o una persona di fiducia nel caso di morte o comunque se qualcosa va storto.



:: Dagli auguri agli addii

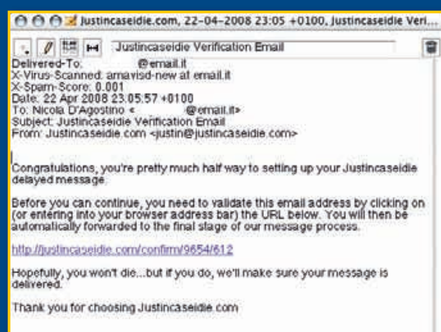
Justincaseidie.com deriva da un progetto molto più ambizioso e molto vecchio nato ben sette anni fa e doveva essere un sistema per comunicare buone e cattive notizie, ricco di funzioni e che avrebbe raggiunto il destinatario non solo via email ma anche tramite SMS o telefonata. Dopo la doccia fredda del dot-boom è nato un progetto più ridotto e terra-terra che fa poco e bene e lo fa anche gratis.
Bastano pochi clic ed un paio di email per attrezzare un messaggio "con la sicura" da usare prima di un viaggio pericoloso. Motivo? Per mandare un'ultima lettera o comunicare informazioni sensibili a chi di dovere se qualcosa dovesse andare storto, che sia la nostra morte o anche solo l'impossibilità fisica di spedire in prima persona.

:: Come funziona

Per usare il servizio basta andare sul sito facendo clic sulla voce "Create" e sulla colonna di sinistra inserire il proprio nome e indirizzo e-mail.



Una volta fatto bisogna controllare la posta dell'account fornito armandosi di un po' di pazienza (nel nostro caso ci ha messo circa venti minuti ad arrivare).


Justincaseidie.com, 22-04-2008 23:05 +0100, Justincaseidie Veri...
Justincaseidie Verification Email
Delivered-To: @email.it
X-Virus-Scanned: amavisd-new at email.it
X-Spam-Score: 0.001
Date: 22 Apr 2008 23:05:57 +0100
To: Nicola D'Agostino < @email.it>
Subject: Justincaseidie Verification Email
From: Justincaseidie.com <justin@justincaseidie.com>

Congratulations, you're pretty much half way to setting up your Justincaseidie delayed message.

Before you can continue, you need to validate this email address by clicking on (or entering into your browser address bar) the URL below. You will then be automatically forwarded to the final stage of our message process.

http://justincaseidie.com/confirm/9654/612

Hopefully, you won't die...but if you do, we'll make sure your message is delivered.

Thank you for choosing Justincaseidie.com

Il messaggio di conferma con link

Il messaggio contiene il link di attivazione che al contempo permette di impostare tutti i dettagli della comunicazione differita.

Check-in Time e Check-In Date sono orario e data in cui, se non si interviene, il messaggio verrà spedito. Segue il nome e l'indirizzo del destinatario e il (breve) testo. A questo punto all'indirizzo usato per attivare il servizio verrà recapitata un'e-mail che fa da conferma, offre il riepilogo e due link per annullare la scadenza o modificare qualsiasi dettaglio.

TORNADO, l'uragano nero

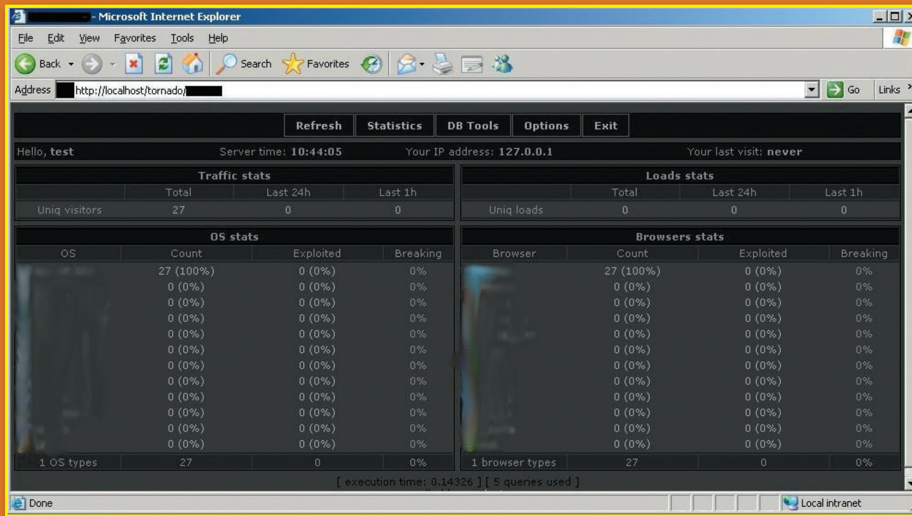
A fine aprile, la casa produttrice di sistemi di sicurezza informatici Symantec ha reso noto di aver scoperto un programma pirata "tutto in uno"

A fine aprile Symantec, la casa produttrice dei sistemi Norton, ha annunciato a gran voce alla stampa la scoperta di un programma denominato Tornado. Un tornado che avrebbe "scatenato una ventata di panico", a detta del produttore di sistemi per la sicurezza informatica. Il programma fa parte della famiglia di Ice Pack e degli altri Mpack, di cui abbiamo parlato in passato. La particolarità di "Tornado"? Sfrutta ben 14 punti vulnerabili dei nostri programmi di navigazione sul Web. Quattordici falle di Internet Explorer, Firefox Mozilla e Opera. Come i suoi cugini dell'Europa orientale, Tornado viene innanzitutto installato su un server Internet. Il pirata ve lo installa in uno spazio Web acquistato con dati bancari contraffatti, oppure direttamente usando un server pirata. Il primo caso è più raro, perché consentirebbe agli amministratori dei siti sfruttati di mettere le mani sul codice sorgente di Tornado. È proprio così che Symantec è riuscita



Status	Exploit	Exploited	Last 24h	Last 1h	Breaking	Loads	Last 24h	Last 1h	Breaking
on		0 (0%)	0	0	0%	0 (0%)	0	0	0%
on		0 (0%)	0	0	0%	0 (0%)	0	0	0%
on		0 (0%)	0	0	0%	0 (0%)	0	0	0%
on		0 (0%)	0	0	0%	0 (0%)	0	0	0%
on		0 (0%)	0	0	0%	0 (0%)	0	0	0%
on		0 (0%)	0	0	0%	0 (0%)	0	0	0%
on		0 (0%)	0	0	0%	0 (0%)	0	0	0%
on		0 (0%)	0	0	0%	0 (0%)	0	0	0%
on		0 (0%)	0	0	0%	0 (0%)	0	0	0%
on		0 (0%)	0	0	0%	0 (0%)	0	0	0%
on		0 (0%)	0	0	0%	0 (0%)	0	0	0%
on		0 (0%)	0	0	0%	0 (0%)	0	0	0%
off		0 (0%)	0	0	0%	0 (0%)	0	0	0%
off		0 (0%)	0	0	0%	0 (0%)	0	0	0%
on		0 (0%)	0	0	0%	0 (0%)	0	0	0%
on		0 (0%)	0	0	0%	0 (0%)	0	0	0%
Totals:	0 active exploits	0 exploited systems			0%	0 loader responses			0%





a mettere le mani su questo programma, solitamente venduto su alcuni forum russi. Una volta installato,Tornado si usa come IcePack. Dopo l'inserimento di un login e di una password, si controlla come un programma Internet di base. Il sistema attende di ricevere i dati inviati da altre pagine. La trappola, infatti, scatta in due fasi. La seconda è piuttosto semplice: il pirata deve installare un codice nei siti preventivamente violati. Il codice ha lo scopo di trarre in inganno i visitatori di questi siti. Ognuno di essi rischierà quindi di essere contagiato dai codici dannosi di Tornado, nella misura in cui è vulnerabile a una delle 14 falle utilizzate dal programma. È un sistema di pirateria che fa furore sulla Rete da diversi mesi. Siti come Monster, Virgin, Reporter Sans Frontière e alcune ambasciate sono stati già toccati dal contagio. Alcuni casi dimostrano che Tornado non è solo e che questa famiglia di programmi pirata non ha ancora terminato di produrre nuovi rampolli. "È semplice" - afferma T0fx, esperto del settore -"Oggi siamo di fronte all'automazione dei programmi pirata. L'intruso installa il programma e poi lascia che sia la tecnologia ad agire. So perfino di casi in cui i pirati ricevono i dati via SMS". I programmi in questione sono venduti a prezzi compresi tra i 100 e i 1.000 dollari, a seconda delle opzioni e delle possibilità… I server infettati possono perfino essere affittati. Insomma, la globalizzazione avanza anche nel mondo dei pirati. "Con questo modello" - spiega Liam O'Murchu di Symantec - "i creatori del programma possono venderlo a pochi clienti di fiducia a un prezzo elevato, invece di distribuirlo a numerosi clienti sconosciuti rischiando di vedere il codice reso pubblico". www.symantec.com/enterprise/security_response/weblog/2008/04/tornado_on_the_loose.html

:: Come ripararsi dal tornado

Attenzione: questo tipo di programma non esce mai allo scoperto per caso. Spesso le versioni più vecchie vengono sguinzagliate nella Rete per motivi molto precisi. "Chi li vende vuole sfoggiare le proprie capacità" - conferma t0fx - "oppure i pirati diffondono la loro creazione per poi mettere le mani su pseudo-pirati che si lasceranno a loro volta infettare". Insomma, Tornado non ha nulla di eccezionale ma dimostra che i pirati tecnologicamente avanzati sono sempre più efficienti. Una delle opzioni di Tornado, oltre a quelle che consentono di infettare i visitatori, di recuperare i cookie e gli IP eccetera, è quella che permette di far credere che il programma non esista. Se ci imbattiamo in un server che ospita Tornado, il nostro browser ci comunicherà un messaggio di errore di connessione. Come proteggerci da questo tipo di attacchi? Anche per chi non ha nessuna conoscenza tecnica è molto semplice difendersi da Tornado e dalla sua banda. Aggiorniamo i nostri programmi di navigazione e il nostro sistema operativo, installiamo un firewall e il gioco è fatto. Anche imbattendoci in una pagina infetta, non correremo alcun rischio.

Verità e bugie... in VISTA





Di sicuro a noi non piace ma dobbiamo ammettere che si dicono anche un sacco di cose non vere sull'Os di Microsoft, facciamo un po' di chiarezza

Da prima ancora della sua uscita, intorno a Windows Vista sono nati miti e leggende in quantità infinita. Alcuni si sono poi dimostrati indovinati, altri solo parzialmente veri e molti assolutamente falsi. Miti che resistono ancora oggi, a più di un anno dall'uscita del sistema operativo, nonostante le smentite sia teoriche sia pratiche. Cerchiamo quindi far luce su questa montagna di mezze verità e intere bugie, indagando sui misteri e sulle dicerie che circondano il sistema operativo Microsoft più chiacchierato di tutti i tempi. Ma come accade anche per le leggende metropolitane prima o poi spunterà qualcosa di nuovo!

Vero

Falso

VISTA SI ESPANDE ALL'INFINITO

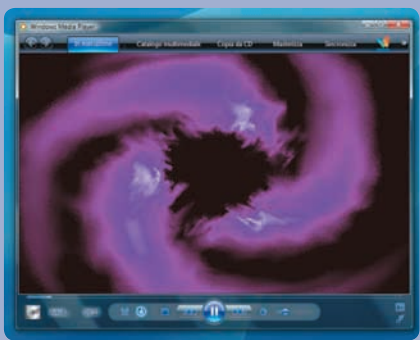
Chiunque abbia installato Vista di persona è testimone di un curioso fenomeno: la cartella di sistema, che al primo avvio occupa circa 8 GB, col passare del tempo può raggiungere e superare i 15 GB. La causa principale è la cartella di sistema Winsxs, destinata ad accogliere tutte le librerie DLL utilizzate dai programmi che installiamo utilizzando Vista. In pratica le nuove applicazioni non sovrascrivono più eventuali DLL già presenti, magari leggermente diverse perché personalizzate dai vari produttori di software, ma in compenso la cartella di Windows è destinata a occupare sempre più spazio e non c'è modo per liberarsene se non con il vecchio sistema tanto caro agli utenti Microsoft, formatta e reinstalla tutto...

VISTA ESAUDISCE OGNI TUO DESIDERIO...

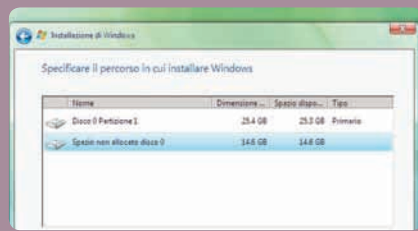
I computer più recenti offrono almeno due core, ovvero due unità di calcolo inserite nello stesso processore. Questa soluzione permette un netto incremento delle prestazioni senza bisogno di alzare la frequenza di lavoro del processore. Esistono ormai modelli Intel con 4 core. Windows Vista consente di differenziare il carico di lavoro per ogni singolo processore con una semplice operazione. Per farlo basta premere contemporaneamente i pulsanti CRTL+ALT+CANC e dalla finestra che compare a video e selezionare la voce Gestione Attività Windows. A questo punto bisogna selezionare la scheda Processi e poi, con il tasto destro del mouse, evidenziare uno dei processi al momento in esecuzione. Scegliamo la voce Imposta affinità... e decidiamo a quale delle unità di calcolo affidare l'esecuzione del processo.

VISTA BLOCCA TUTTO CIO' CHE È ILLEGALE

In Vista il sistema di gestione dei DRM, ovvero dei diritti di utilizzo dei file audio e video acquistati online, è identico a quello di Windows XP. Ne viene che qualunque contenuto riproducibile su XP è ugualmente accessibile su Windows Vista. Windows Media Player 11, però, è in grado di leggere i contenuti in alta definizione nei formati HD DVD e Blu-ray degradandone il segnale qualora il monitor e la scheda video non siano compatibili con la tecnologia HDCP. Si tratta di un requisito di qualunque lettore per l'alta definizione, imposto dalle case cinematografiche, al quale Microsoft si è dovuta adeguare per forza per ottenere le licenze necessarie.



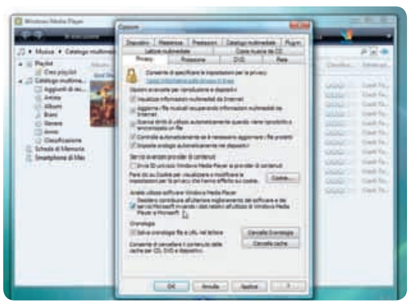
VISTA SI ATTIVA SOLO UNA VOLTA E SU UN UNICO PC



La cosiddetta licenze retail di Vista, ovvero quella che si compra nei negozi separatamente da altri prodotti, si può installare e riattivare quante volte si vuole proprio come capitava con Windows XP. È però necessario rimuoverle dal computer su cui erano installate in precedenza. In altre parole, possiamo cambiare il nostro computer quante volte vogliamo e riattivare la nostra copia di Vista regolarmente acquistata, purché smettiamo di usarla sul vecchio computer. Ciò non vale per le licenze OEM, rilasciate in abbinamento a un singolo computer: in questo caso, il nostro diritto all'uso di Vista è intimamente legato a quella macchina. Non è quindi possibile installarla su una nuova macchina: dovremo acquistare una nuova licenza.

MICROSOFT CONTROLLA OGNI AZIONE ESEGUITA CON VISTA

Ecco una leggenda metropolitana che accompagna qualsiasi prodotto Microsoft, da Windows 98 in avanti. Diverse versioni di Internet Explorer, di Office e di Windows Update sono state più volte accusate di inviare di nascosto a Microsoft informazioni personali e sui programmi installati. Una simile attività non è però mai stata dimostrata e sarebbe del tutto illegale: se Microsoft dovesse effettivamente raccogliere questi dati, difficilmente potrebbe impiegarli a suo vantaggio in una causa legale. È invece vero che alcuni programmi, come Windows Media Player, raccolgono informazioni vitali per il proprio funzionamento dopo aver avvertito l'utilizzatore in modo chiaro ed esplicito.



ANCHE CON VISTA SI POSSONO COPIARE I DVD

Alcuni programmi per duplicare DVD e CD, soprattutto quelli protetti, installano dei driver proprietari per accedere in modo diretto al masterizzatore. Al momento del rilascio delle prime beta di Vista, questi driver non funzionavano correttamente poiché erano stati scritti per altri sistemi operativi. Col passare dei mesi, però, tutte le società che producono software di backup hanno aggiornato i propri prodotti per essere compatibili con Vista. In definitiva, è ancora possibile effettuare le copie di sicurezza dei propri CD e DVD originali, esattamente come con Windows XP.



ACADEMIC, A 99 EURO, COME HOME PREMIUM

La versione Academic di Windows Vista corrisponde esattamente a una versione Home Premium e, per tanto, condivide con la medesima gli stessi programmi e le stesse funzionalità. Questa affermazione, dunque, potrebbe avere un fondo di verità soltanto confrontando l'offerta Academic con le versioni Enterprise e Ultimate di Windows Vista, molto più costose ma pensate per una tipologia di pubblico molto differente. Cambiano, questo sì, i termini di vendita: anche se molti rivenditori chiudono un occhio e alle volte anche tutti e due, solo gli studenti e gli insegnanti avrebbero il diritto di acquistare questa versione di Vista.

CON LE DIRECTX 10 I GIOCHI SONO PIU' LENTI RISPETTO A XP

Da tempo sbandierate come il futuro dei videogiochi, le DirectX 10 incluse soltanto in Windows Vista non hanno saputo mantenere le promesse e si sono rivelate spesso più lente e pesanti delle versioni precedenti. Le schede video compatibili con queste librerie ci hanno impiegato molti mesi a imporsi sul mercato e, ancora oggi, sono pochi i titoli concepiti per sfruttarle adeguatamente. Solo i costosi modelli di fascia alta, inoltre, hanno garantito prestazioni accettabili. La situazione sta fortunatamente migliorando, ma resta sempre pur vero che gli stessi giochi, quando vengono eseguiti in modalità DirectX 9 su XP, di solito sono più veloci.

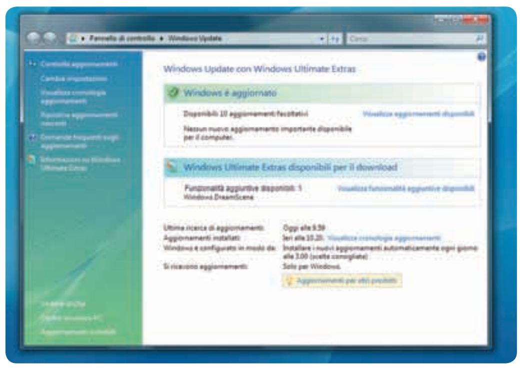


WINDOWS MAIL COME OUTLOOK EXPRESS

Windows Mail è soltanto l'ennesima evoluzione del programma Outlook Express, rimasto sostanzialmente invariato dall'uscita di Windows XP. Non è dunque un programma del tutto nuovo, come alcuni sostengono, ma solo la nuova versione di un vecchio programma.

IL SERVICE PACK 1 INTEGRA GLI AGGIORNAMENTI PRECEDENTI

Quando Microsoft rilascia un Service Pack, di solito questo comprende tutti gli aggiornamenti rilasciati in precedenza per mezzo di Windows Update. Non solo: spesso nei Service Pack vengono incluse anche nuove caratteristiche e nuovi programmi, in grado di modificare pesantemente il sistema operativo stesso.



VISTA CONSUMA DI PIU'

Nonostante un sistema di gestione del risparmio energetico rinnovato, Vista è destinato a consumare più energia elettrica rispetto a XP. Le cause principali sono il motore grafico Aero e i servizi di indicizzazione e di SuperFetch. Queste sono le componenti che pesano più di tutte sui consumi energetici di un portatile. I produttori stanno ovviando all'inconveniente ricorrendo a batterie più efficienti e a tecnologie di memorizzazione innovative.



INCOMPATIBILI?

La maggior parte dei programmi a 32 bit, scritti per le versioni precedenti di Windows, funzionano anche sulla versione a 64 bit di Vista. In molti casi i malfunzionamenti non sono dovuti alle applicazioni ma a driver di sistema ancora immaturi. Esiste poi una piccola percentuale di programmi che, per un motivo o per l'altro, sui sistemi operativi a 64 bit non possono proprio funzionare. Sono comunque destinati a scomparire con la diffusione costante dei sistemi a 64 bit.

COSA VUOLE AERO?

Per far funzionare il motore grafico Aero integrato in Vista è sufficiente una scheda video pienamente compatibile con le librerie DirectX 9, vale a dire una Radeon 9550 o superiore, oppure una GeForce 5600 o superiore. Altri processori grafici prodotti da altre marche, come Via e Intel, sono ugualmente compatibili. L'importante è che tra le caratteristiche del processore grafico sia presente il supporto ai pixel shader in versione 2.0, caratteristica comune a tutte le schede video uscite negli ultimi anni.

Attacco "grafico"



Un informatico francese presenta su Internet un affascinante studio sulla violazione di una password in formato MD5 mediante una combinazione di CPU e scheda grafica

Su Internet si trova una miriade di sistemi che consentono di violare una password codificata in MD5. L'idea di Benjamin Vernoux, alias Titan, non è quella di essere il più astuto del mondo ma di valutare e studiare un metodo che utilizzi le risorse dei nostri computer. Vernoux ha appena realizzato un piccolo strumento che consente di "craccare" una password in formato MD5. "Ho impiegato tre giorni per realizzarlo"- rivela Benjamin - "per creare un modello privo di interfaccia grafica è stato necessario circa un giorno; l'adattamento a MFC e l'ottimizzazione hanno richiesto circa due giorni". Perché questo progetto? "Semplicemente per il gusto della sfida e per cercare un'ottimizzazione definitiva dell'accoppiata processore/scheda grafica." - spiega Vernoux - "Mi sono tornati in mente i vecchi tempi della programmazione su Amiga con Copper/Blitter… la programmazione era ottimizzata e i programmi e i giochi erano estremamente rapidi e reattivi, sull'esempio di AmigaOS, che per me è tuttora un punto di riferimento in termini di reattività di un sistema operativo".



La prima versione beta del programma creato dallo studio di Titan sfornava circa 20 milioni di hash MD5 al secondo, senza alcuna ottimizzazione particolare; solo l'algoritmo MD5 è stato convertito per CUDA 1.1 (GPU) in modo da operare in parallelo. Il funzionamento è piuttosto innovativo. Per quanto riguarda il processore, il sistema effettua un calcolo "brute force" (36 possibilità, con le lettere dalla a alla z più le cifre da 0 a 9) e prepara l'MD5 con un risultato di 64 bit per password. "Questo calcolo viene effettuato per blocchi di 2 milioni di password (cioè 128 MB)" - spiega Benjamin. Il programma copia le password di tipo MD5 sulla memoria GPU (Graphic Processing Unit), cioè la scheda grafica. La GPU calcola l'algoritmo MD5 di ciascuna password e verifica se l'HASH corrisponde a quello da individuare. "Se l'hash viene individuato, viene messo un flag a 1 e l'hash individuato, trasferito nella memoria GPU, viene quindi verificato dal processore".

Dopo varie ottimizzazioni del generatore "brute force" sul lato CPU, con una "riscrittura completa dell'algoritmo brute force in funzione delle dimensioni della password", sul lato GPU il creatore del programma è passato a 30 milioni di hash MD5 al secondo. La versione 0.1, offerta sul sito Internet di Benjamin Vernoux, ha subito un'ottimizzazione



della banda passante. "Le password calcolate sul lato CPU vengono archiviate a 16 bit invece che a 64 bit e viene utilizzata la memoria CPU CUDA in modalità pinned, del 20% più veloce. La modalità normale si aggira intorno ai 2,1 GB al secondo, la modalità pinned è sui 2,5 GB al secondo". La versione 1.0 è caratterizzata inoltre da un'ottimizzazione dell'algoritmo MD5 sul lato GPU, con "l'utilizzo di vettori per il caricamento delle password in blocchi di 128 bit con eliminazione dei conflitti". La prossima fase del lavoro di questo informatico consisterà nell'esecuzione di gran parte del calcolo "brute force" nella GPU, che ha una banda passante di oltre 47 GB al secondo su una GeForce 8800GT, "mentre la banda passante della memoria CPU è solo di 2,5 GB al secondo circa". Ecco dunque un eccellente studio informatico che interesserà agli appassionati della codifica e della criptazione. La versione attuale del programma effettua un calcolo "brute force" su 36 caratteri (le lettere dalla a alla z più le cifre da 0 a 9). Il programma e lo studio sono disponibili sul sito http://bvernoux.free.fr/md5/index.php

Ma quanto ti chiamo... Ma quanto mi costi

Ci siamo inoltrati tra i meandri delle tariffe di telefonia mobile per scoprire qual è quella ideale per i nostri lettori, ecco i risultati



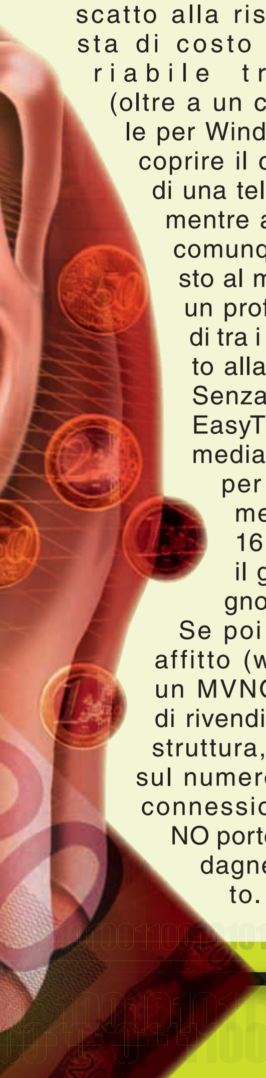
A seguito delle liberalizzazioni imposte e richieste dal mercato stesso, gli operatori mobili al pari di quello che è successo nel settore fisso hanno dovuto rendere disponibili le proprie reti a soggetti nuovi, che possono rivendere i servizi voce e dati al pubblico senza essere proprietari dell'infrastruttura. Scelta motivata dal fatto che la risorsa utilizzata (l'etere) è limitata e non permetterebbe un'assegnazione ulteriore di frequenze con le tecnologie attuali, oltre a tutto ciò che conseguirebbe l'introduzione di una nuova infrastruttura sul territorio (impatto ambientale, riassegnazione frequenze, permessi dai vari enti, ritardi burocratici e costi di ogni tipo).

Ma pur saturo dal punto di vista infrastrutturale, il mercato è sempre interessato alla concorrenza e l'ingresso di molti nuovi soggetti quali gli operatori mobili virtuali (Mobile Virtual Network Operator, MVNO) non può che rappresentare un fattore positivo per i consumatori, anche se poi va comunque analizzata la convenienza delle loro offerte. In Italia, si sono fatti avanti soggetti prima totalmente estranei al mercato delle TLC come i gruppi della grande distribuzione (Carrefour, COOP, Auchan, Conad), alcuni bancari (Poste, Acotel) e chiaramente anche operatori già presenti nel mercato. Stanno infatti per partire o sono già partite in alcuni casi, le offerte sul mobile di Tiscali e Fastweb e gruppi stranieri come British Telecom e non mancano comunque gruppi industriali che cercano comunque di cavalcare l'onda di queste nuove opportunità anche solo a livello di sponsorizzazioni, come Autostrade SpA. Ci si aspettava di conseguenza una concorrenza basata sostanzialmente sui prezzi mentre al contrario gli operatori virtuali che già sono partiti si sono praticamente uniformati alle tariffe preesistenti, una situazione sicuramente determinata dalla giovane età degli MVNO nostrani, ma anche dal costo delle interconnessioni.

Si stima infatti a livello europeo che le tariffe di interconnessione (ossia il costo che ogni gestore dovrebbe pagare

al concorrente per telefonate tra le loro reti) sia di 3,5cent/min. Proprio in questi giorni l'Autorità per le garanzie nelle comunicazioni, ha stabilito che il costo attuale dovrà convergere entro il 2011 a 5,9cent/min per TIM-VODAFONE-WIND (dai circa 9cent/min attuali) e 7cent/min per TRE (dai 13cent/min attuali), quindi mantenendo un ampio margine di guadagno. Ma se si guarda poi alle tariffe che vengono offerte agli utenti, non ci sono praticamente casi di costi inferiori a 4cent/min (es. Wind4) a cui comunque viene applicato uno scatto alla risposta di costo variabile tra 12-16 cent (oltre a un canone di 4€ mensile per Wind4). Basta lo scatto a coprire il costo per l'operatore di una telefonata di 4-5 minuti mentre a noi viene applicato comunque un (ulteriore) costo al minuto. Se prendiamo un profilo tariffato a secondi tra i migliori e senza scatto alla risposta (es. SuperSenzaScatto, VeloceCoop, EasyTIM), verifichiamo immediatamente che il costo per minuto è incredibilmente alto: stiamo sui 16-17 cent/min. Quindi il gestore ha un guadagno netto del 50%!!!

Se poi l'operatore cede in affitto (wholesale) la rete a un MVNO, diventando quindi rivenditore anche dell'infrastruttura, oltre a guadagnare sul numero maggiore di interconnessioni (dato che il MVNO porterà nuovi clienti) guadagnerà anche con l'affitto. Ma tenendo tariffe di interconnessione elevata, il MVNO non potrà essere così competitivo e in alcuni casi non ci sarà effettivo vantaggio (sulla carta) a scegliere un MVNO piuttosto che un gestore reale (come nell'esempio, tra WIND e CoopVoce). Come possiamo difenderci? Se si ha già una propria sim e un proprio piano tariffario, magari datato, il consiglio spassionato è quello di tenerselo stretto pur confrontandolo con le nuove offerte. Questo perché si potrebbe trattare di piani tuttora convenienti o comunque adeguati alle proprie esigenze. Quindi non cedere alle lusinghe di nuove offerte e in questo caso magari provare la nuova tariffa con un'altra sim. Se invece siamo decisi ad attivare un nuovo piano tariffario, prima di tutto va analizzato il traffico medio che si genera, valutando in particolare quante ore/mese di telefonate facciamo a prescindere dalla rete di destinazione (anche perché con la portabilità del numero non c'è più l'associazione tra un prefisso e un gestore) e qual è la spesa tipica mensile (tra ricariche e traffico). Una volta stabilito questo monte ore e il budget, vanno analizzati i costi cercando di capire se effettivamente si chiamano



MVNO	Gruppo	Rete usata
CoopVoce	COOP	TIM
in partenza	NOVERCA (ACOTEL)	TIM
in partenza	TISCALI	TIM
UNO Mobile	CARREFOUR	VODAFONE
PosteMobile	POSTE ITALIANE	VODAFONE
Conad INSIM	CONAD	VODAFONE
BT Mobile	BT Italia Spa (ex-Albacom Spa)	VODAFONE
A-Mobile	AUCHAN	WIND
Telepass Mobile	AUTOSTRADE per l'Italia	WIND
in partenza	ASTELIT	TRE
Daily Telecom Mobile	Daily Telecom	TRE
in partenza	FASTWEB	TRE
in partenza	PLDT	TRE

Reti MVNO

	Dal 1°/7/08 (dal 1°/9/08 per TRE)	Dal 1°/07/2009	Dal 1°/07/2010
Telecom Italia	8,85	7,70	6,60
Vodafone	8,85	7,70	6,60
Wind	9,51	8,70	7,20
TRE	13,00	11,00	9,00

Costi di interconnesione

Operatore	Profilo	Scatti o Secondi	Scatto	Verso gruppo	Verso stessa rete	Verso Altri operatori	Verso fissi	Sconto estero	AutoRicarica	Osservazioni
TIM	EasyTIM	Scatti 60s	0,00	16/min						
TIM	Easy TIM Mega Autoricarica	Scatti 60s	0,00	16/min					5/min (max 30€/mese)	Opzione Autoricarica gratuita se contestuale a attivazione sim
TIM	TimTribù Vitamine	Secondi	0,00	25 + 0/min	19/min					Scatto (vitamina) applicato alla prima telefonata della giornata
TIM	TimTribù Base	Scatti 30s	16,00	9/min	19/min					
TIM	TimTribù 1 Eurocent	Scatti 30s	16,00	1/min	19/min					Canone di 5€/mese
TIM	TimTribù 5 Eurocent	Scatti 30s	16,00	5/min	19/min					
TIM	TIM CLUB Prepagati	Secondi	0,00	9/min	19/min					
TIM	TIM Base	Secondi	0,00	9/min	30/min					
TIM	TIM Welcome Home	Scatti 30s	19,00	9/min		19/min		Da 3/min a 24/min		Non c'è scatto per telefonate verso l'estero
VODAFONE	You&Vodafone New	Scatti 30s	16,00	9/min		19/min				Tariffa 15cent/min solo verso 47 paesi One Nation
VODAFONE	Vodafone Tempo Libero	Secondi	0,00	16/min						15cent/min solo dalle 18.00 alle 08.00 ogni giorno e 24 ore su 24 il sabato, la domenica e i giorni festivi per 30gg dopo una ricarica
VODAFONE	Vodafone Zero Limits	Scatti 30s	19,00	0/min (senza canone 19/min)		19/min				Canone di 2€/settimana
VODAFONE	Vodafone Tutti	Scatti 60s	16,00	12/min (senza ricarica 19/min)						Necessaria ricarica mensile da 15€
VODAFONE	Vodafone Facile Small Ricaricabile			400minuti/mese (oltre 19/min)		19/min				Canone di 19€/mensili e solo con carta di credito
VODAFONE	Vodafone One Nation New	Scatti 60s	16,00	15/min				15/min		Tariffa 15cent/min verso 47 paesi One Nation
WIND	SuperSenzaScatto	Secondi	0,00	17/min						
WIND	Wind 12	Scatti 30s	16,00	12/min					5/min (PienoWind) 3/sms (PienoSMS)	PienoWind 4€/6 mesi; PienoSMS 4€/6 mesi
WIND	Wind 4	Scatti 30s	16,20	4,8/min (4/min+IVA)						Canone di 4€/mese
TRE	Super7	Scatti 60s	16,00	15/min					5/min, 2/sms	Necessaria ricarica mensile
TRE	Super10	Scatti 60s	16,00	15/min					10/min, 5/sms	Per le autoricariche è necessaria una ricarica mensile
TRE	Super 0 Mondo	Secondi	16,00	0/min		15/min	0/min	Da 1/min a 15/min		Senza ricarica 0/min → 15/min
CoopVoce	SuperFacile Coop	Scatti 30s	12,00	12/min						Lo scatto include 5 secondi di telefonata
CoopVoce	Tariffa Veloce Coop	Secondi	0,00	17/min						
CoopVoce	Carta Servizi Più Valore Coop	Scatti 30s	10,00	10/min						Acquistabile con punti Coop e valida 3 mesi
PosteMobile	Con Tutti	Scatti 30s	0,00	16/min						
PosteMobile	Con Noi	Scatti 30s	0,00	6/min		22/min		Da 8/min a 16/min		No scatto verso estero "Con il mio paese"; Integrazione con PostePay e BancoPosta
PosteMobile	Con Tutti Premium	Scatti 30s	0,00	6/min		16/min				
Conad InSim	Conad Insieme	Scatti 60s	12,00	6/min		12/min	6/min			
A-Mobile	A-Mobile	Scatti 30s	15,00	10/min						

Riepilogo dei piani

sempre i soliti numeri (fidanzata/o, famiglia, amici) nel qual caso potrebbe anche convenire far migrare tutti verso profili che scontano le chiamate "in casa" (una TimTribù, You&Vodafone, Super 0 Mondo) o con un canone fisso (tipo NoiWind e GenteDi3) che abbatterebbero i costi di queste telefonate, peggiorando quasi sicuramente quelle meno frequenti verso altri numeri. Nel caso peggiore, in cui le telefonate siano comunque destinate verso tutte le numerazioni, va ricercata una tariffa flat, ossia con lo stesso costo verso tutti i numeri 24h/24h e possibilmente senza canoni (vincoli di ricarica o abbonamenti). Profili di questo tipo hanno generalmente lo scatto alla risposta e quindi sono poco convenienti per chiamate brevi, mentre su chiamate lunghe riescono a "spalmare" il balzello.

Come si vede però in ognuna di queste situazioni risulta che l'offerta è sempre insoddisfacente perché va a penalizzare comunque l'uso prolungato. Se la spesa mensile si aggira tra i 30 e i 50 euro, può convenire sensibilmente passare a un profilo a canone mensile in versione ricaricabile (in modo da evitare i costi di un abbonamento reale: costi di apertura, tassa di concessione governativa, bolli sulle fatture, ..), dove si è vincolati ad effettuare una ricarica mensile a fronte di un pacchetto di minuti verso tutti. Essenzialmente le tariffe possono essere divise tra profili a scatti e profili tariffati a secondi. In modo molto grossolano, i primi sono più convenienti per telefonate medio-lunghe (superiori comunque a 1-2 minuti) mentre i secondi sono migliori per telefonate corte, anche di qualche secondo.

Successivamente alla rimozione del





costo delle ricariche, gli operatori hanno provveduto a rimodulare verso l'alto i costi dei nuovi piani tariffari o applicando altri costi sui profili esistenti (ad es. aggiungendo servizi non richiesti che hanno generato un generale malumore). Questo perché ovviamente dopo anni di introiti maggiorati, iniziavano a perdere guadagni così consistenti. Caso opposto è quando il gestore offre un credito virtuale maggiore di quello pagato (es. ricariche della Coop e in passato le ricariche Power della TRE): in tal caso si abbassa percentualmente il costo per singola chiamata a patto che non si sia vincolati a chiamare un'unica direttrice (es. solo numeri fissi e/o solo numeri dello stesso gestore). Altri vincoli, che stanno sparendo, sono quelli relativi a tariffe legate alla fascia oraria per cui ho un costo molto basso in ore della giornata meno congestionate (es. la sera) e un costo elevato nella restante parte. Un'altra variabile interessante è quella legata poi a meccanismi di autoricarica: il gestore concede all'utente una provvigione sul guadagno che gli fa entrare in cassa. Paradossalmente, più si ricevono telefonate da gestori diversi più si viene compensati da un credito virtuale che cresce, ma che può essere speso solo in telefonate e servizi del medesimo gestore. In questo campo la tariffa principe (non più commercializzata, ma ancora acquistabile su eBay e forum) è stata SuperTuaPiù della TRE che permetteva di ricaricarsi di 10cent ogni minuto entrante e 4cent ogni sms entrante senza limiti per traffico proveniente da reti diverse da TRE.

A Settembre 2007, la tariffa è stata rimodulata unilateralmente dal gestore dimezzando queste ricariche e rendendo l'AutoRicarica che prima era senza scadenza un bonus da consumare entro 60gg dall'erogazione con un massimale di 5000€ mensili. C'è chi tuttora non ha necessità di ricaricare il telefonino (se non per evitare la scadenza annuale della sim) avendo una discreta cifra "residua" come credito telefonico; sicuramente l'unico modo certo per combattere l'esosità dei gestori telefonici. In questo momento sono commercializzati con questa filosofia solo EasyTIM Mega Autoricarica e Super7/Super10 (ricarica obbligatoria); sui piani WIND si possono attivare PienoWIND/PienoSMS (canone mensile) e sui piani VODAFONE si può attivare Ricaricami (canone mensile). Nel caso ottimale, si potrebbe pensare di ammortizzare mensilmente i costi di un canone fisso (es. GenteDi3) con il credito erogato come autoricarica, ma i gestori non permettono di pagare più i servizi con questi bonus. Mediamente però la spesa mensile viene abbattuta perché comunque si usa tale bonus per traffico abituale.

Nelle tabelle sono indicati i profili che sembrano più vantaggiosi e i costi da evitare assolutamente, anche se ciò che è adeguato per un utente, non necessariamente è la soluzione migliore per un altro e da verificare sempre con quanto realmente commercializzato. Alcuni consigli: chi preferisce un profilo con costi più bassi verso un gruppo o solo lo stesso operatore, prenda in considerazione le ricariche con bonus (Coop aggiunge 10% fino a settembre, Vodafone il 20%, MaxiRicarica TIM il 33% circa) che virtualmente riducono il costo per singola chiamata. Sui piani senza scatto, la scelta è tra EasyTIM (opz. Autoricarica) e Con Tutti/Tutti Premium. E sembra vincere TIM, dal momento che si può usare la MaxxiRicarica e ci si autoricarica fino a 30€ mensili. Ma con PosteMobile viene offerta la possibilità di gestire operazioni di pagamento dal telefonino (bollettini, telegrammi) oltre a gestire direttamente la carta di credito PostePay e il conto BancoPosta se si è titolari.

Chi invece vuole un profilo generico, può scegliere tra SuperFacile Coop (su rete TIM, scatto 12cent inclusivo di 5 secondi e 12cent/min) e A-Mobile (su rete WIND, scatto 15cent e 10cent/min). Per entrambi sono previste promozioni di credito regalato facendo la spesa senza canoni o obblighi di ricarica. A breve partiranno altri MVNO (Tiscali, Noverca, Fastweb) per cui è sperabile che ci sia maggior concorrenza per il traffico nazionale e per l'estero che ci sia con la concorrenza dovuta a offerte dedicate agli stranieri in Italia da parte di DailyTelecom, Astelit, PLDT e gli altri che verranno.

Massimiliano Brasile



CONOSCI IL TROJAN HORSE

Arrivano sotto forma di normali programmi e ne combinano di tutti i colori. Sono i Cavalli di Troia...



I "Trojan Horse" ("cavalli di Troia"), dei quali sono in circolazione oltre un migliaio di esemplari (comprese modifiche e varianti), sono una categoria di virus relativamente nuova e forse del tipo più pericoloso fra quelli comparsi in tempi recenti. I Trojan Horse minacciano tra l'altro di sopraffare i sistemi che usano solo programmi anti-virus e firewall per difendersi. Questi virus hanno ormai raggiunto un livello di sofisticazione tale da costituire una seria minaccia per qualsiasi utente che non abbia preso serie precauzioni per difendere i propri dati.

::Un po' di storia

Il nome deriva da un episodio della mitologia greca avvenuto dopo che i Greci avevano stretto d'assedio per oltre dieci anni la città fortificata di Troia. Fingendo di ritirarsi, l'esercito lasciò davanti alle porte della città un cavallo di legno che nascondeva al suo interno un drappello di uomini. Gli abitanti di Troia furono convinti da una spia a portare il cavallo all'interno delle mura e nottetempo gli infiltrati approfittarono della loro posizione per spalancare le porte della città. L'esercito greco irruppe, massacrando gli abitanti per poi saccheggiare e dare alle fiamme la città. In un contesto informatico, il "cavallo di Troia" è un programma malevolo che si installa facendo finta di essere un altro software. Spesso si tratta di programmi legittimi al cui interno un pirata informatico ha nascosto un virus, uno spyware o, più spesso, una backdoor cioè un programma che permette a un pirata di prendere il completo controllo di un computer tramite il collegamento Internet.

:: Programmi molto pericolosi

Questo tipo di virus è stato progettato inizialmente come strumento di auto-espressione da parte di abili programmatori: i danni causati dai primi "cavalli di Troia" si limitavano a blocchi del computer, comportamenti anormali o al limite alla perdita di dati del computer dell'utente. Oggigiorno, invece, i Trojan vengono usati per lo più in modo da installare una backdoor e consentire a un utente remoto di avere accesso al computer della vittima a insaputa di quest'ultima. Ottenuto questo risultato, l'intruso può usare il computer per qualsiasi fine, esattamente come l'utente. Solitamente l'obiettivo dell'intruso è esaminare il disco fisso della vittima per scoprire se contiene del materiale prezioso. Questo può essere costituito da ogni sorta di documenti: per esempio ricerche preziose, informazioni su carte di credito o password di accesso a siti Web riservati. Se individua un documento di valore, l'intruso può copiare i dati in questione sul suo disco fisso esattamente come l'utente legittimo può copiare un file su un dischetto. Quel che è peggio, tutte queste operazioni avvengono all'insaputa dell'utente, che mentre si verificano può trovarsi seduto davanti al computer impegnato a elaborare un documento completamente diverso. Il fatto che il disco fisso lavori senza alcuna ragione apparente può essere l'unico indizio che segnala che sta avvenendo qualcosa di imprevisto. L'intruso può inoltre creare il caos nel sistema eliminando dei file (di sistema), cancellando dati preziosi o nella peggiore delle ipotesi cancellando tutto il disco fisso. Per farlo può essere sufficiente aggiungere un comando al file autoexec.bat, che viene eseguito ogni volta che Windows parte.

TUO NEMICO

TUO NEMICO

La volta successiva in cui la vittima ignara avvierà il computer, verrà lanciato automaticamente il comando di formattazione del disco. L'uso di una password non garantisce alcuna protezione, perché tutti i Trojan odierni sono in grado di registrare i tasti digitati dalla vittima e di trasmettere l'informazione all'intruso. Le password possono quindi essere decifrate dal Trojan e perfino modificate al fine di impedire all'utente di accedere ai suoi stessi file!

:: In che modo un Trojan infetta il computer?

Perché un intruso possa avere accesso a un computer, la vittima deve essere indotta a installare espressamente il Trojan. Il sistema più comune consiste nell'offrire un programma apparentemente utile o anche un videogioco gratuito nel quale è nascosto il Trojan. Installando il programma, installiamo anche il Trojan. Le cause di infezione più comune sono:

- Permettere a un "amico" di accedere al computer in assenza dell'utente.

- Avviare file ricevuti tramite un qualsiasi programma di messaggistica come ICQ.

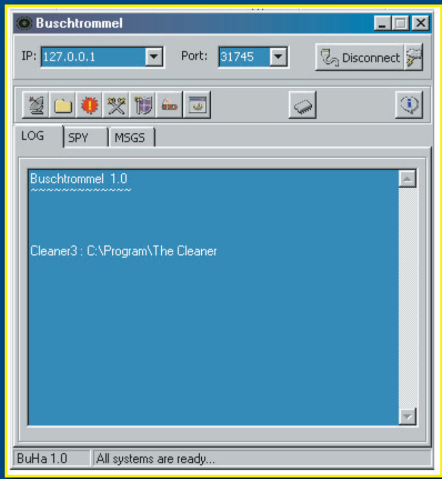
- Aprire un allegato di posta elettronica proveniente da un mittente sconosciuto.

- Avviare file di qualsiasi tipo provenienti da fonti sospette o sconosciute.

Quasi tutti i Trojan sono composti da due elementi principali. Si tratta del "server" e del "client". È il server a infettare il sistema dell'utente. Una volta infettato, il computer è accessibile a qualsiasi utente remoto, solitamente definito intruso o "cracker", che dispone della parte client del Trojan. Gli intrusi possono setacciare Internet alla ricerca di un utente infetto (tecnicamente, l'aggressore invia pacchetti di richiesta a tutti gli utenti serviti da uno specifico fornitore di accesso a Internet). Trovatone uno (cioè quando la parte server del virus che si trova sul computer infetto risponde alla richiesta della parte client), l'aggressore si collega al computer in questione e crea un "collegamento" tra esso e il suo computer, come in una normale conversazione telefonica. Effettuata questa operazione (che può richiedere in realtà anche solo pochi secondi), l'intruso avrà accesso completamente illimitato al computer dell'utente e potrà farne qualsiasi cosa desideri. L'intruso diviene cioè il padrone e l'utente il suo schiavo, perché a meno di disconnettersi da Internet e più in generale dalla rete l'utente è assolutamente indifeso e non ha alcun mezzo per difendersi da questo attacco.

:: Liberi tutti

A questo punto può effettuare qualsiasi azione accessibile a noi stessi. Per esempio, se conserviamo i dettagli della carta di credito sul computer, l'intruso può impadronirsi di queste informazioni. Non necessariamente l'intruso userà personalmente la carta di credito ma potrebbe vendere l'informazione a terzi che a loro volta potranno abbandonarsi ad acquisti folli a spese nostre. L'intruso può inoltre rubare password allo scopo di avere accesso a informazioni riservate o a siti Internet protetti. Inoltre può far riavviare o spegnere il computer senza preavviso, aprire il lettore di CD-ROM, cancellare file, aggiungerne di nuovi, usare il programma di posta elettronica e altro ancora. Le possibilità sono infinite. L'intruso può controllare, organizzare ed effettuare qualsiasi operazione sul computer infetto, come se si trovasse fisicamente seduto davanti a esso.



Il "lato utente" di un Trojan è una semplice applicazione che permette di connettersi e disconnettersi dal computer remoto che si desidera controllare.

:: Accesso privilegiato ai disonesti

Un Trojan Horse assomiglia alla porta di servizio di una casa (in maniera simile ai backdoor, programmi nocivi dal funzionamento analogo ai Trojan). Se la si lascia aperta, chiunque può entrare in casa e impadronirsi di qualsiasi cosa alle spalle del proprietario. La differenza è che una "porta di servizio" installata su un computer consente a chiunque di entrare e di impadronirsi dei dati, cancellare file o formattare il disco fisso anche quando l'utente è presente. Niente segnala in modo visibile che sta avvenendo qualcosa di insolito, se non il fatto che il disco fisso stia funzionando all'impazzata senza ragioni apparenti.